DIPLOME: the single source of truth on comparability and qualification certifications.

DIPLOME: the single source of truth on comparability and qualification certifications.

Public Version: 1.18

Last Update 20th May 2019

Luca Lantero and Pietro Marchionni
Introduction

THE CONCEPT

The «Diplome» service aims to create a world-wide ecosystem where the qualifications and certifications of an individual are safely and securely managed, reducing risks of falsifications thus facilitating the portability process of such certifications. In a few words, within Diplome, individuals get assigned a secure “wallet” where they can store their certifications using blockchain technology, therefore creating a decentralised, transparent, certified and tamper-proof ecosystem with the goal to simplify the procedure for a student, a graduate or a professional to enrol in a university or to apply for a job in the labour market.

Diplome’s Blockchain-based service is primarily focused on INDIVIDUALS.

Diplome is built on 6 main key pillars:

1. Diplome is citizen-oriented
2. Diplome is free of charge
3. Diplome is based on open technologies
4. Diplome does not force organisations to use a specific technology but adapts to those in place
5. Diplome does not control user identity but is open to any external identification system
6. Diplome is fully compliant with all metadata included in already existing Bologna and EU instruments (Europass documents, Diploma Supplement, etc.)

The concept of certifications is not limited to final qualifications issued by educational institutions (school leaving qualification, VET diplomas, higher education degrees, etc.) but is open to handle:

- Diplomas
- Degrees
- Certificates
- Transcripts
- Final examination results
- Diploma Supplements
- Temporary certificates
- Professional qualifications
- Professional licenses

To map the above typology of certifications, a complete data model (ontology) has been developed with the widest compatibility with existing models. This concept and the related data model can easily be extended to new areas where certification issuance is required for both an individual or a company and such certification would have to be shared with third parties. To give an example we can think of a SME desiring to share its Quality Certification with a client to fulfill a contract requirement.
The system therefore implements a global network of trust and is open to:

- **the holder of the qualification**: unique owner of the information, who can upload free of charge all the qualifications of his/her academic career in his/her wallet;
- **higher education institutions**: will be able to use the ecosystem in all the phases of an academic career. From the enrolment stage, through the entire study programme, to registering the exams taken and the corresponding marks, up to the awarding phase, when the final qualification will also be registered in blockchain in a tamper-resistant and immutable way. The qualifications and the information registered in blockchain remain at the student’s disposal for his/her entire academic and professional career;
- **stakeholders awarding non-academic qualifications**: certificates attesting a new training programme can be uploaded into the student’s wallet;
- **certification authorities**: stakeholders that assess qualifications, such as a country’s ENIC-NARIC or credential evaluation centres, can provide information about transparency, authenticity, comprehensibility and comparability of qualifications at an international level directly in blockchain.

Future enhancements will include the following usage cases:

- **corporations**: corporations that need a secure and trusted ecosystem to store certificates attesting their compliance with specific regulations (e.g. a construction SME holding an Employee Safety and Security certificate)
- **IOTs**: devices performing some actions that need to store certificates attesting their compliance with specific regulations (e.g. a speed camera or a building temperature sensor)
- **goods**: products that need to guarantee to the buyer compliance with regulations (e.g. CE compliance of a motorbike helmet, or the yearly check of a building elevator)

**WHY BLOCKCHAIN?**

Blockchain is a technology that is at the basis of the Diplome service and allows the secure storage and sharing of the qualification data owned by the user, in particular this technology supports the service in the following areas:

1. **Digitalization of the recognition process**: blockchain technology facilitates and speeds up the process of recognition of qualifications simplifying the trusted distribution of verified certifications and at the same time reducing fraud.

2. **Student-centred approach**: holders of the qualifications are the main stakeholders of the system. They can upload documents of their academic career, choose who they want to share them with and certify their competences in a standardised way in line with international standards.

3. **Data security and privacy**: the holder of the qualification is the only owner of the information and of the crypto key that constitutes the only way to access user data, being fully compliant with the principles of data privacy, e.g. General Data Protection Regulation (GDPR).

4. **Fraud minimization**: data saved within the blockchain structure is tamper-resistant (sometimes defined as ‘immutable’) and any modification of stored information is complex to be implemented, with a cost that does not match the potential advantage. Access to the information registered in blockchain by a certified source allows the direct verification of the authenticity of the qualification stored.
THE KEY STAKEHOLDER: CIMEA

CIMEA is the official Italian centre within the NARIC - National Academic Recognition Information Centres – network of the European Union and the ENIC - European National Information Centres – network of the European Council and of UNESCO. Since 1984, CIMEA (Information Centre on Academic Mobility and Equivalence) has performed its focused activity of information and advice on the procedures of qualifications recognition and on themes linked to Italian and international higher education and training. CIMEA supports academic mobility in all its forms and owns an international document centre and specialised databases on foreign higher education systems, on the types of qualifications of every country and on the national legislation in terms of higher education.

CIMEA’s Credential Information Service – CIS, is a credential evaluation service of certification and comparison of Italian and foreign qualifications, with a view to rendering qualifications increasingly more comprehensible and recognizable in a national and international context.

CIMEA has decided to utilize the power of blockchain technology to digitalise the process of recognition of qualifications (based on Lisbon Recognition Convention principles) and because the Credential Information Service - CIS asks for student-related tamper-resistant documentation erasing any possibility of falsification of given certificates and qualification information.

The DIPLOME ecosystem

Diplome’s approach is to create an interlaced distributed network of information that allows the precise identification of the certification of any participating holder thus automating the process of Credential Information Services, certifying by design the authenticity of the stored information.

This can be achieved with a modern distributed technology and strategic approach that takes success stories from other markets or solutions and adapts them successfully to the certification ecosystem utilizing the latest technologies such as Blockchain and Artificial Intelligence.

Diplome together with CIMEA and other key partners has defined usage cases, identified key requirements and designed a system that will revolutionize the certification process simplifying the trusted distribution of verified certifications and reducing fraud.

Diplome represents a real change in the qualification ecosystem, bringing the ultimate tool to guarantee each party of the trustworthiness and authenticity of the information stored. Within this framework, students, universities, certification authorities, public entities and corporations can share and have access to a unique data store that is built by a decentralized trust network of certified entities that reduces the friction in education and business thus reducing costs for all participating actors.

IS THIS REALLY NEEDED?

Mobility in work and study is growing daily and there’s a key need in eliminating barriers limiting such sound processes.

This situation has been internationally recognized:

a) the Ministries of the 48 countries participating in the European Higher Education Area have declared within the last Communiqué of the European Higher Education Area (Paris Communiqué):

[…] We also urge the adoption of transparent procedures for the recognition of qualifications, prior learning and study periods, supported by interoperable digital solutions. […] To further promote student
and graduate mobility, we welcome and support initiatives such as the digitalisation of the Diploma Supplement, and commit to support higher education institutions to pursue further student data exchange in a secure, machine-readable and interoperable format, in line with data protection legislation. […] We call on the BFUG to take the issue of digitalization forward in the next working period. […]

b) At the same time, the European Parliament Resolution of the 25th October 2018 on promoting automatic mutual recognition of diplomas declared:

[…] whereas improving recognition procedures for higher education and upper secondary education diplomas and for the outcomes of learning periods abroad is a prerequisite for the establishment of a European Education Area […] Calls on the Member States to make a political commitment and put in place mechanisms for the automatic mutual recognition of higher education and upper secondary education qualifications, as well as the outcomes of learning periods abroad, in line with the objectives of the European Education Area; […] Asks Member States to increase transnational cooperation and to make use of new technologies in order to increase efficiency, reduce costs, improve transparency and build trust to that end, with a view to taking advantage of the educational and job opportunities stemming from the internal market […]

c) Finally, the Council of the European Union has recently approved on 26th November 2018 the “Recommendation on promoting automatic mutual recognition of higher education and upper secondary education and training qualifications and the outcomes of learning periods abroad” where it is clearly stated to:

[…] Explore, in cooperation with Member States, the potential of new technologies, such as blockchain technology, to facilitate automatic mutual recognition. […]

Diplôme aims to address the highlighted needs, in practice:

Diplôme supports automatic mutual recognition of academic and professional qualifications, improving efficiency in the recognition process and reducing at the same time costs for citizens and the Public Administration.

Key Service elements

The Diplôme service must guarantee that data stored within the system is handled appropriately while enforcing the strictest models of privacy and security handling.

In particular the following elements have been carefully handled within the ecosystem:

1. DATA QUALITY
   - All data stored in the chain is provided by authorized certified entities. Information source and subject are tightly bound and registered with the data.

2. DATA PORTABILITY
   - Complete data interoperability has been implemented: we have defined an extensive and common ontology for qualifications and represented it with an open JSON format that can be easily imported into other systems.

3. SECURITY
   - With an innovative approach to data exchange, information stored is protected throughout the whole flow with cross-cryptographic techniques.
4. **MINIMIZATION**
   - On-chain data can be stored with different models and structured in a way that represents the minimum amount required to provide **secure and reliable information** about the qualification.

5. **CONTROL**
   - Data owner has **full control** of his/her own wallet and stored data, directly driving the entire process and is the only player allowed to handle and where needed share stored information.

6. **OPENNESS**
   - The whole system is open to any willing participant (certification authorities or end users) without any entry barrier. Data access is not handled through a Diplo service and once allowed by the data owner, information is always shared with an **open and standardized** approach.

Diplo also aims to be in line with the newly developed standards related to Decentralized Identifiers (DIDs), under the full control of users. DIDs are widely used in Diplo to handle the issued qualifications and certifications that follow the Verifiable Claims approach under development by W3C.

**Overall Structure**

Diplo is a service that, even if based on **blockchain technology**, aims to provide a simple and frictionless interface to any participating entity.

The service is composed of four building blocks:

1. **the front-end layer**: the user interface whose aim is to avoid any impact on usability by utilization of well-established technologies and a captivating UX

2. **the back-end layer**: the middleware service engine based on open technologies, that runs and integrates the blockchain and AI subsystems with the user interface, decoupling the two from their specific and sometimes contrasting characteristics

3. **the infrastructure layer**: the blockchain-based interoperable and accessible service where information is securely stored guaranteeing data protection and portability

4. **the management layer (enterprise network)**: the management interface used by all players that run and manage the certification services
The Diplome blockchain ecosystem relies on a third-party open permissioned blockchain and implements on top of that a safe network where every stakeholder will participate in building up the ecosystem based on its role.

We have to this purpose identified the following main stakeholder groups:

1. **Certification Authorities**: these are the entities/organisations that issue certifications (e.g. a University) or entities that provide cross/additional certification services (e.g. NARICs). The two different certification authorities have different permission schemes while sharing a similar final objective, i.e. the issuance of a certified document.

2. **Users**: these are the service users that receive certifications from Certification Authorities. Users may or may not also be part of an organization (e.g. university, professional registry, etc.) that can also be a Certification Authority.

3. **Validators**: this is a service control function that guarantees overall stability of the service. The main validation process is now handled by Diplome’s Oracle Service whose aim is to guarantee that the issuer is an entity allowed to issue certificates. Enquiries about the Oracle Service are open to anyone. In Diplome’s ecosystem, validators are different from the infrastructure validators, that are specific nodes of the blockchain whose aim is to formally validate the performed transaction without checking the details of the issued certification.

4. **Governing Body/bodies**: these are the entity/entities that execute the governance tasks of the system. These tasks are related to logical infrastructure management as for example the maintenance of the Oracle Service, the update of the service smart contracts, the addition of a new validator, etc.

In future, as the overall system evolves, other types of stakeholder will be added with different profiles: for example there could be non-organizational certifiers, e.g. service users (not organisations) that are entitled to certify other users due to their proven experience in some areas/fields.
Certification Authorities are further divided into ‘Direct Certification Authorities D-CA’ that are entitled only to certify users belonging to their organisation (e.g. Universities) unless specifically required by a user and ‘Cross Certification Authorities C-CA’ that are entitled to certify every user within the Diplome network (e.g. NARICS).

Each of the stakeholders has specific permissions on the network based on their entitlement built on the above structure.

In cases where an organisation already has its own network or digital management system an appropriate gateway will guarantee interoperable exchange of information between the organisation network and Diplome.

Users, when part of Diplome, are assigned an account within the blockchain that will represent their ‘wallet’ holding a set of smart contracts that will act as a secure repository for every certification issued by a Certification Authority. At the time of setup a password and a Key Pair (Public,Private) is generated and provided in order to enable the user to exercise full exclusive control over the wallet and data saved in the connected smart contracts.

The address of the account is effectively a decentralized identifier (DID), aimed eventually at providing a standard way for our users and organisations involved in the certification process to possess a permanent, unique, cryptographically verifiable identifier entirely under the identity owner’s control.

A simplified logical depiction of the DIPLOME ecosystem can be found here below:

We can depict the whole education history related to a user and available within Diplome, with the following diagram:
Considering that every player in Diplome’s ecosystem (i.e. every DIS) has an associated public-private key-pair, Certification Authorities are able to digitally issue and sign a qualification or certificate built with the concept of verifiable claims.

As any entity receiving the certificate from the user would be able to obtain the DID of the issuing CA that is part of the transaction and of the payload itself, the verification of the signature on the claim is transparent and accessible eliminating therefore any possibility of tampering.

Diplome does not aim to manage a certified identity system for its users as identity management is not part of any certification management workflow: in fact, identification of the user is supposed to happen externally to Diplome’s solution while easily integrated. Nevertheless, Diplome may provide its own light registration process that has been designed in a way that can be easily integrated or even replaced by an external certified Identity Management solution as for example a Self Sovereign Identity framework or a government-certified framework such as EIDAS in the EU.

Whenever the user personally, his/her organisation or a cross certification authority adds a certificate, a dedicated smart contract is activated: the task of this smart contract is to verify that the appropriate
permissions (e.g. organisation, user information, etc.) and data structure (e.g. appropriate organisation signatures) are used together with consistent metadata (e.g. this certification is not in conflict with other certifications).

Upon success the smart contract owned by the user account loads the data structure related to the issued certification and enforces specific user-controlled access to it. The validation of the consistency of the data (not on the content of such data) is performed by the user-owned smart contract in conjunction with Diplome’s oracle service. In time, the user account will be enriched by continuous certified data inflow, so as to create the overall ‘Education Scheme’ related to the user’s achievements:

![FIGURE 5 USER EDUCATION BLOCKCHAIN ACCOUNT SCHEME](image)

Such a scheme is key both for study continuation/evolution and for any recruiter interested in a candidate’s profile that is trusted and verified.

**Qualifications management**

Diplome is agnostic in the specifics of the qualifications that can be issued by a certification authority, but for the sake of implementing a fully interoperable ecosystem, an issued qualification is supposed to belong to a certain category.

The categories identified by Diplome are the following:

1. Secondary School qualification
2. Higher Education qualification
3. VET (Vocational Education and Training) qualification
4. Professional qualification

Other categories are in the process of being added to handle certifications issued to corporations or devices (IoT).

To give an example, a secondary school final examination certificate will belong to the first category while a Higher Education Diploma Supplement will belong to the second.

Naturally any certificate within Diplome is represented by its metadata as for example the qualification’s awarding body name or the issue date. Each of the categories therefore implicitly imposes a flexible, pre-
defined data structure for its representation within the Diplome ecosystem: this allows wide portability while ensuring consistency and the interoperability of stored qualification information.

Within a user’s wallet, when issued by an authorized CA, the above qualification structure is represented in JSON format to maximise portability both vs. automatic importing services and vs. exporting to any other digital storage systems.

Diplome is currently built on a standard Ethereum blockchain and can run on any ethereum-based variants.

The actual running Diplome runs on an Ethereum Quorum implementation managed by the Alastria consortium.

For further information on Alastria please visit their official website: https://alastria.io/en/

Building blocks

Diplome’s blockchain ecosystem is based on three building blocks:

USER’S WALLET

Diplome’s user wallet is composed of a standard user blockchain address/account and one or more smart contracts each handling one or more qualifications. There can be several smart contracts as each of them can handle qualifications based on a pre-defined Profile: there are therefore up to 3 smart contract types even though the structure can be extended in future following further models.

ORGANISATION’S WALLET

An organisation issuing a qualification must hold a blockchain address/account connected to an Org-SmartContract with specific characteristics required to identify the organisation and its permission types. Only an Org-SmartContract can add a qualification to a user’s wallet.

DIPLOME’S ORACLE

One of the key governance processes of Diplome is the one that allows external and independent verification of whether an entity is a certified authority in Diplome’s ecosystem. Anyone can query Diplome’s oracle to verify if a specific organisation is part of Diplome’s network.

The certified qualification is saved within Diplome's ecosystem in a logical layered structure where the top layer is open for public access and contains general information used to provide origin certification and verification of the data stored. The other layer, encrypted, contains the certification qualifying metadata that can be disclosed only by utilising the private key belonging to the user.

Once data is shared by the user with a third party, there’s a strong need for the receiving entity to have an independent way to verify that such data is that which is effectively saved within Diplome’s ecosystem also in order to avoid man-in-the-middle issues. This is because as all data is not openly accessible during verification a user or a third party may utilize external methods to modify the data while sharing.

The top layer (open to everybody but limited to entities with specific information) is therefore used to guarantee that anyone accessing the stored data directly can directly verify that the data has the following information present in it:
1. Issuing entity
   - This allows to independently and securely verify that the certification issuing entity is the same as the one indicated within the certificate itself

2. Owner Address/Public Key
   - This allows to independently and securely cross-verify that the certification receiving user is the same as the one indicated within the certificate itself

3. Certification payload hash
   - This allows to securely verify that the certificate data shared by the user is the same as that saved within the issued certificate

Other information is used for internal verification (e.g. Timestamp and Smart Contract version).

The following image depicts the structure just described above:
Certification Process

Once an Organisation (already part of Diplome) decides to issue a new certificate (or a digital version of an existing one) to a user, a complex process enforces and validates all required steps necessary to create a new metadata structure to be saved within the user’s wallet.

To ensure data protection and increase security of the overall process, the metadata structure going to be saved within the certificate’s data block is signed with a double logical process:

1. it is encrypted with the private key of the issuing Certification Authority
2. the resulting data is again encrypted with the user’s public key

We have the situation therefore that after data is saved within user’s wallet, the only way to share such data in a usable format is to:

1. Decrypt the data with the User’s private key
2. Decrypt the resulting data with the Certification Authority Public Key

This double steps ensures the following:

- Data can be shared exclusively by the owner as we need to have his private key
- Data encryption implicitly contains the identification of the issuing CA
- In the case that a CA loses its key, such loss would not affect existing certificates and in case of issuance of a new certificate, all existing ones would not need to be changed/reissued

The process of sharing the data is then further verifiable by using the annexed public header information accessible to everyone but requiring key information to limit possibilities to have uncontrolled access or of DOS attacks.

The previously described process is implemented and verified by Diplome’s back-end through Diplome’s Smart Contracts.

The various Smart Contracts that form part of Diplome’s ecosystem have the duty to ensure that the previous process is duly followed and that all participants in the process are verified entities.

Entities wishing to issue a new certification are verified by the Smart Contract through a specific request to an external oracle handled by Diplome as its governance duty: this oracle holds the list of approved certification authorities and is checked in several steps of the certification issuing and sharing process.

Content of a Certificate when issued is under full control of the issuing Certificate Authority that from Diplome’s point of view is responsible also for the protection of its private key used in the certificate issuing process. After a certificate has been issued, control is exclusively in the hands of the receiving user.

In case of needs of modification, rejection or any other change in the issued certificate a new verification must be issued by the same Certification Authority with an updated serial number. This information will be handled during the shared verification process to guarantee that only the last version of the certificate will be issued by the users.
**DATA PROTECTION PROFILES**

Diplome aims to be a worldwide solution inasmuch as the data protection approach is flexible in order to accommodate different legislations.

Every single organisation part of Diplome is free to choose any of the profiles that have been identified in order to match the different requirements set by an organisation participating to the ecosystem.

At the moment 3 data protection profiles are included in the design:

**Profile 1**

The data structure representing the issued qualification is completely anonymized and no personal data (or data related to personal data) is stored within the Diplome wallet, while only the signature of the qualification is present on the blockchain structure. An external qualification digital document referenced by the signature stored on the user's blockchain account would be needed to complete the qualification certification process. This profile guarantees GDPR compliance.

**Profile 2**

The data structure representing the issued qualification is completely anonymized and protected with double encryption using the qualification organisation key and user key. The full JSON representation of such a qualification is stored within the blockchain user account. No identity data is stored within the qualification dataset. This profile guarantees GDPR compliance.

**Profile 3**

The data structure representing the issued qualification is completely anonymized and protected with double encryption using the qualification organisation key and user key. Identity data is stored in the wallet (i.e. SSI reference) together with the qualification representation in JSON format that includes full details of the qualification. This profile guarantees GDPR compliance in case the SSI layer is GDPR compliant as well.

**DATA PROTECTION APPROACH**

Regarding data protection, Diplome follows the PrivacyByDesign and PrivacyByArchitecture approaches. To this end, to implement the appropriate rights management, the wallet created by a user at the time of registration is fully owned by the user him/herself, meaning that the data held by the wallet or related smart contracts within the blockchain network can be freely managed by its rightful owner for his/her own personal use as part of his/her willingness to have a certified and immutable copy of received qualification. Based on this design principle we can for example deduct that the handling of such data falls under the household exemption of the GDPR.

As smart contracts are part of the Diplome solution it is ensured that specific functions that can be called (executed) exclusively by the Certification Authorities and can be used for the benefit of the service provision.

The wallet’s public keys or addresses on a blockchain may be considered personal data: such addresses and keys are under the full control of the user and the data stored in the related wallet and smart contracts are unreadable without the user’s explicit actions.
Diplome cannot handle or modify any stored information even at the user’s request. As the service is designed to guarantee maximum protection of personal data, the following design principles are built in within the logic:

**DATA MINIMIZATION**

The only data saved within the blockchain structure is the key metadata required to provide trusted information about the academic subject.

**ACCURACY & QUALITY**

All data saved within the user wallet and smart contracts, related to the user’s qualification, come exclusively from entitled and verified Certification Authorities. The Certification Authority unique signature is saved within the data structure itself, creating an unbreakable and trusted link between the data and its source.

**DISCLOSURE LIMITATION**

Once stored within the user’s wallet and smart contract, all data related to any certified qualification is in full control of the user him/herself, and only he/she can give access rights to or disclose such data. This allows for example the provision to the user of full Rights to Access, Restriction of Processing, Objection to Processing and Erasure. In fact, the Right to be Forgotten can be simply implemented by the user through three methods:

1. Temporarily denying access to any stored data through a “Deactivate” function implemented directly into the smart contract. At any time the user can “Reactivate” it restoring full functionality.
2. Definitively ‘cancelling’ the data through the “Destroy” function implemented in the smart contract: this function is not reversible and therefore the user won’t have the possibility to use the service for that specific container anymore. Other contracts containing other data may still be used.
3. Erasing the crypto keys that constitutes the unique way to access the user’s functions and data: in this way the user with all related contracts will be no longer be accessible and no reversibility will be possible.

**OPENNESS AND PORTABILITY**

All data saved within the user’s account can be exported in a standardised format allowing the user full portability of such data to any other system or service. The data structure follows the open-standard and language-independent JSON format, therefore compatibility is guaranteed with any modern IT system. This design approach therefore guarantees full Right to Data Portability to Diplome users.

**ACCOUNTABILITY**

As per the data accuracy section, data is linked uniquely and indissolubly to its source (Certification Authority). Full details on the specific event that created such data are also saved at the same time (e.g. timestamp, source details, etc.). Data access, based on the owner’s permission, is also logged to trace any possible misuse.

**INFORMATION SECURITY**

As per blockchain intrinsic characteristics, once data is saved within the chain, it becomes tamper-resistant (immutable) and any modification becomes impossible even for system administrators. Access to the data is restricted to the wallet’s owner through cryptographic keys.
**REVERSAL RISK**

All data related to a qualification is stored within the wallet with a double encryption and any reference to external data is furthermore saved in a Salted Hashed format. This technique will guarantee non-reversibility of stored information even considering the indications of ARTICLE 29 DATA PROTECTION WORKING PARTY (0829/14/EN WP216) as it refers to single “attribute value”, while in Diplome the Encryption plus Salt&Hashing is run on the full metadata set that is composed of several and structurally different attribute-values.

Diplome aims to extend its capabilities with functionalities that will give access only to a subset of the stored data giving therefore powerful tools to the end user to share only the information needed to perform the service he/she requires. For example, he /she can share only the date of the issuing of the qualification or the final score.

**CONCLUSION**

Diplome is a new way to handle certifications designed to address challenges in the student and mobility area and designed to be extended to new areas such as Corporate, devices or IoT certification.

Diplome presents significant growth opportunities to government bodies, certification authorities, corporations and end users in ways that have never existed within the current industry.

Diplome’s team is already working to create new assets and extensions that will make the service grow while always maintaining a user-centric concept, in line with the decentralised model of DLT/blockchains.

Diplome is **SIMPLE, SECURE** and **CERTIFIED**:

**SIMPLE:** with Diploma, qualifications are always at hand and it is possible to choose who to share them with in a simple and secure way.

**SECURE:** the qualifications saved in Diplome on blockchain are immutable and unchangeable, protected from any possible interference, and can be shared and verified in a secure way. Using blockchain it is possible to verify with certainty the authenticity of a qualification, minimizing the risk of fraud. Diplome is structured to guarantee the security of personal data and protect the privacy of the title holder, in line with the principles of the European General Data Protection Regulation (GDPR).

**CERTIFIED:** Diplome is an open ecosystem, which institutions, bodies, authorities, and all those who in various ways release or certify qualifications and competences can join. Diplome is a private permissioned blockchain, the type best suited to the public sector, a space in which only the "certifying" agents can operate, guaranteeing the reliability and security of the ecosystem.