# DIPLO-ME

## WHITE PAPER

DIPLO*ME*: the single source of truth on comparability and qualification certifications.

*Document Version 1.50*

*Last Update 25th November 2019*

# DIPLO-ME

## WHITE PAPER

### Introduction

#### THE CONCEPT

The service **«diplo*me*»**, aims to create a world-wide ecosystem where the qualifications and certifications of an individual are safely and securely managed, reducing risks of falsifications and facilitating the portability process of such qualifications.

In few words, within Diplo*me*, individuals get assigned a secure wallet where they can store their qualifications using the *blockchain technology*, therefore creating a **decentralized, transparent, certified** and **tamper-proof ecosystem** with the goal to simplify the procedure for a student, a graduate or a professional to enroll in a university or to apply for a job in the labor market of another country.

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

There are thus, 6 main key pillars on which Diplo*me* is build on:

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

The concept of qualification is not limited to titles issued by educational institutions (high school diploma, university level diploma etc) but is open to handle:

- ✓ Secondary school titles
  - Diploma
  - Transcript
  - Final Examination
  - Etc
- ✓ High School titles
  - Diploma

- Transcript
- Diploma Supplement
- Temporary Certificates
- Etc

✓ VET (Vocational education and training)
- Diploma
- Transcript
- Etc

✓ Professional Qualifications

The actual data model is extensible to new areas where qualification issuance is required for both an individual or a company and such qualification is needed to be shared with specific entities; to give an example we can think at a SME willingly to share its Quality Certification with a third party.

The system implements a **global network of trust** and it is open to:

- **holder of the qualification:** unique owner of the information, can upload free of charge all the qualifications of his academic career in his wallet;
- **higher education institutions**: will be able to use the ecosystem in all the phases of the academic career. Since the enrolment stage, through the entire study programme, to register the exams taken and the corresponding marks, till the awarding phase, when also the final qualification will be registered in blockchain in a temper resistant and immutable way. The qualifications and the information registered in blockchain remain at the student disposal for his entire academic and professional career;
- **stakeholders awarding non academic qualifications:** certificates attesting a new training programme can be uploaded in 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, understanding and comparability of qualifications at international level directly in blockchain.

Future enhancements may include the following entities:

- **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 compliancy of a motorbike helmet, or yearly check of a building elevator)

**Why *blockchain?***

Blockchain is a technology that is at the basis of Diplo*me'*s service and allows to securely store and share the qualification data owned by the used, 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 frauds.
2. **Student-centered approach:** holders of the qualifications are the main stakeholders of the system. They can upload documents of their career, choose with whom they want to share them and certify their competences in a standardized 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's data, being fully compliant with the principles of the data privacy, e.g. *General Data Protection Regulation (GDPR)*.
4. **Fraud minimization**: data saved within the blockchain structure are temper 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 to verify directly the authenticity of the qualification stored.

***THE KEY PARTNER: 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 advisory 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**, 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 digitalize the process of recognition of qualification** (based on Lisbon Recognition Convention principals) and Credential Information Service CIS asking student related documentation temper-resistant erasing any possibility of falsification of given certificates and qualification information.

## The DIPLOME ecosystem

Diplo*me*'s approach is to create an interlaced distributed network of information that allows to precisely identify the certification of any participating user thus automating the process of Credential Information Services, certifying therefore 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 as *Blockchain* and *Artificial Intelligence*.

Diplo*me* together with CIMEA and other key partners has defined use cases, identified key requirements and designed a system that will revolutionize the certification process simplifying the trusted distribution of verified certifications and reducing frauds.

Diplo*me* represents the real change in the qualification ecosystem, bringing the ultimate tool to guarantee each party of the trustfulness 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 healthy process.

This situation has been internationally recognized, for ecample the Ministries of the 48 countries referring to the European Higher Education Area declared:

[…]

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.

[…]

At the same time, the European Parliament resolution of 25 October 2018 on promoting automatic mutual recognition of diplomas 2018/2838(RSP) 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;

[…]

The Council of the European Union has recently approved 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 is clearly stated to:

[…]

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

**Diplo*me*** aims to address these needs:

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

## Key Service elements

Diplo*me* must guarantee that data stored within the system is handled appropriately and 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 are provided by certified entities. Information source and subject is bound and registered with the data
2. **DATA PORTABILITY**
   - Complete data interoperability have been implemented: we defined an extensive and common ontology for qualifications and represented it with an open JSON format that can be easily imported in other systems.
3. **SECURITY**
   - With an innovative approach to data exchange, information stored is **protected** through the whole flow with cross-cryptographic techniques
4. **MINIMIZATION**
   - On-chain data can be stored with different models and structured in a way that represent the minimum amount required to provide **secure and reliable information** about the qualification. Data can also be stored off-chain based on issuer/receiver decision.
5. **CONTROL**
   - Data owner has **full control** of his own data and of the entire process and is the only player allowed to disclose stored information.
6. **OPENNESS**
   - The whole system is open to any willingly participant (certification authorities or end users) without any entry barrier. Data access is not handled through a Diplo*me* gatekeeping service and once allowed by data owner, information is always shared with an **open and standardized** approach.

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

## Overall Structure

Diplo*me* 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 backend layer***: the middleware service engine 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 actors that run and manage the certification services

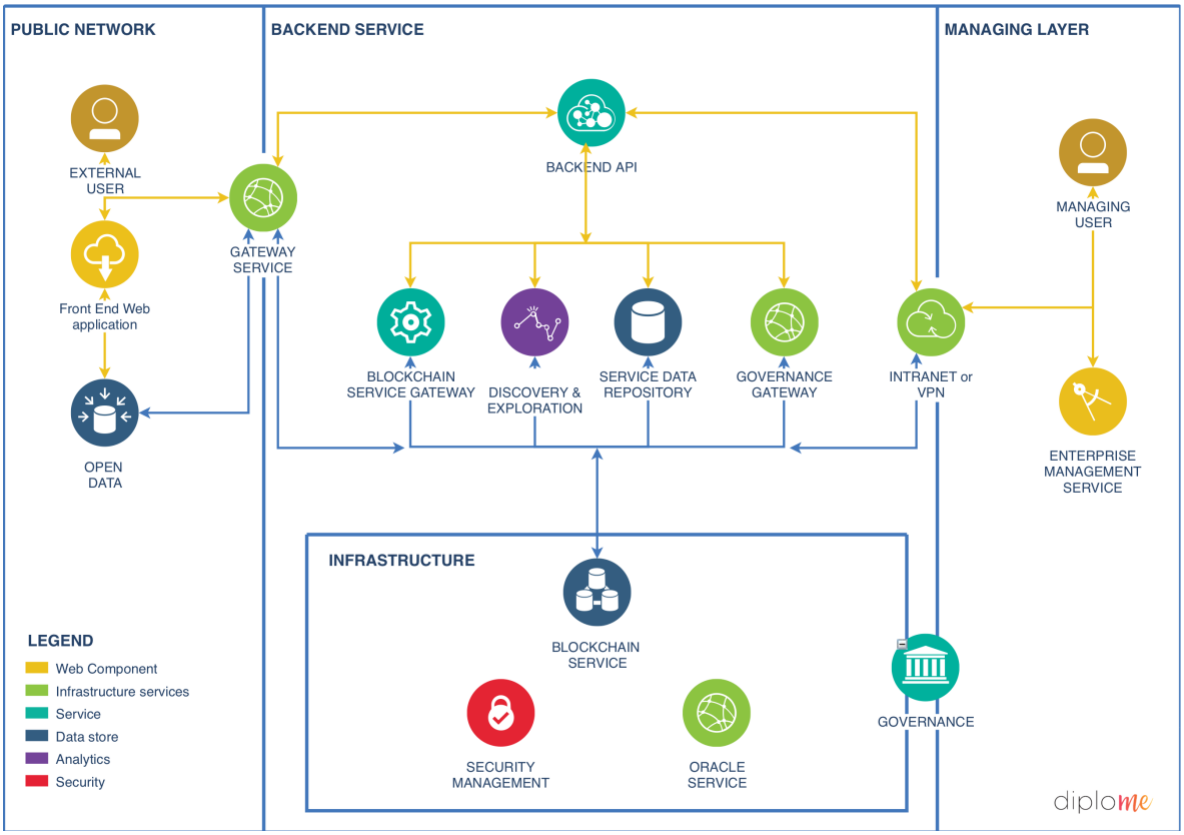


FIGURE 1 - LOGICAL STRUCTURE

The Diplo*me* blockchain ecosystem relies on a private permissioned blockchain and implements on top of it a safe network where every stakeholder will participate to building-up the ecosystem based on its role.

We have at this purpose identified the following main stakeholders groups:

1. ***Certification Authorities***: these are the entities/organizations that issue studies 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 certificate.
2. ***Users***: these are the service users that receive certifications by Certification Authorities. Users may or may not also be part of an organization (e.g. university, professional registry, etc) that can be also a Certification Authority.
3. ***Validators***: these constitute the nodes of the blockchain infrastructure and their aim is to formally validate the performed transaction without checking the details of the issued certification. Another validation process is handled by Diplo*me*'s Oracle Service that verifies that the qualification issuer is an entity allowed to issue certificates.
4. ***Governing Body/ies***: 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, when the overall system will evolve, other types of stakeholder will be added, for example there could be non-organizational certificators, e.g. service users (not organizations) that are entitled to certify other users due to their proven experience in some areas/fields or corporate users.

Certification Authorities are further divided in '**Direct Certification Authorities D-CA'** that are entitled only to certify users belonging to their organization (e.g. Universities) unless specifically required by a user and '**Cross Certification Authorities C-CA'** that are entitled to certify every user within the Diplo*me* network (e.g. NARICS).

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

In case an organization has already its own network or digital management system an appropriate gateway will guarantee interoperable exchange of information between the organization network and Diplo*me*.

Users, when registered within Diplo*me*, are assigned an account within the blockchain that will represent their wallet holding a set of smart contract that represent the repository for every document related to their education. Together with the account a Key Pair (Public,Private) is generated and provided as well in order to enable the user full control over data saved into the wallet and related smart contracts.

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

A simplified schematic depict of the DIPLOME ecosystem can be find here below:

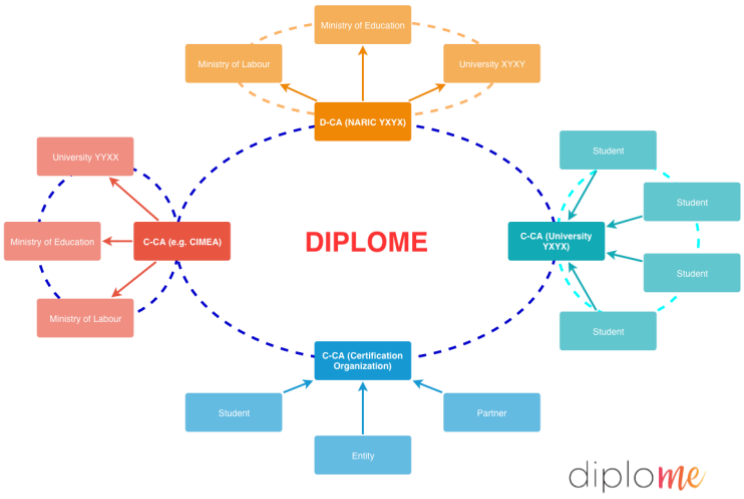


FIGURE 2 DIPLO*ME* MODEL

We can depict the whole education history related to a user and available within Diplo*me*, with the following diagram:

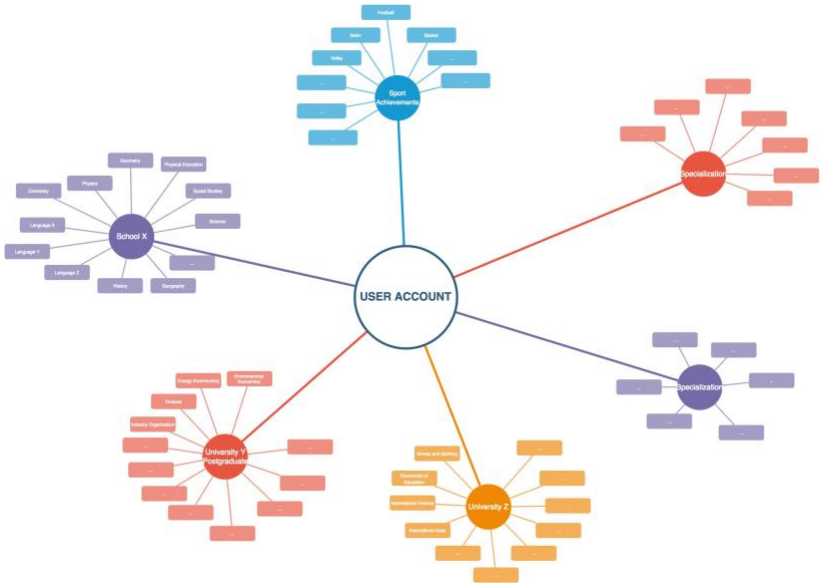


FIGURE 3 USER QUALIFICATION DIAGRAM

Because every actor in Diplo*me*'s ecosystem (e.g. every DIS) has an associated public-private key-pair, Certification Authorities are capable to digitally issue and sign a qualification or certificate built with the concept of verifiable claims/credentials.

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.


FIGURE 4 - CLAIM PROCESS

Diplo*me* does not aim to manage a certified identity system for its users as identity management in not part of any diploma management workflow: in fact certified identification of the user is supposed to happen externally to Diplo*me*'s solution while easily integrated.

Indeed Diplo*me* has 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 as EIDAS in EU.

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

On success the smart contract owned by the user account loads an appropriate data structure related to the issued information and allows specific user-controlled access to it.

Here comes the task of the Validators that verify and guarantee from formal point of view, that this transaction is valid. Naturally this validation does not involve the content of the certification as the task is deemed to the issuing organization. The validation of the consistency of the data (not on the content of such data) is thus performed by the user-owned smart contract in conjunction with Diplo*me*'s oracle service.

Through time, user account will be enriched by continuous certified data inflow, so to create the overall 'Education Scheme' related to user's achievements:

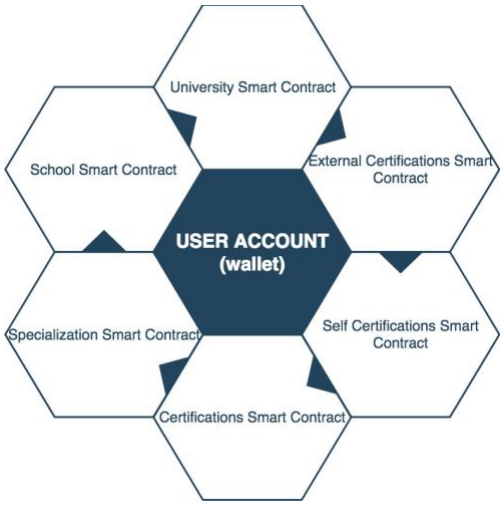


FIGURE 5 USER EDUCATION BLOCKCHAIN SCHEME

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

## Qualifications management

Diplo*me* is agnostic of 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 has to belong to a certain category.

The categories identified by Diplo*me* are the following:

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

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 qualification within Diplo*me* is represented by its metadata as for example the qualification's awarding body name or the issue date. Each of the qualification categories therefore implicitly imposes a flexible, pre-defined data structure for their representation within the Diplo*me* blockchain: this allows wide portability while ensuring consistency and interoperability of stored qualification information.

Within this structure, some metadata may be mandatory (e.g. the Diploma Name or the Student Name) while other data may be optional (e.g the Document Number of the number of Credits issued).

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

Diplo*me's* actually utilize a standard Ethereum blockchain and can run on any ethereum-based variants. The launch of diplo*me* will happen on a Quorum implementation managed by the Alastria consortium.

Diplo*me*'s blockchain building blocks are:

*User's Wallet*

Diplo*me's* user wallet is composed by a standard user blockchain address/account and one or more smart contracts each handling one or more qualifications. There can be more 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.

*Organization's Wallet*

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

*Diplome's Oracle*

One of the key governance processes of diplo*me* is the one that allows external and independent verification if an entity is a certified authority in diplo*me*'s ecosystem. Anyone can query diplo*me*'s oracle to verify if a specific organization is part of diplo*me*'s network

The certified qualification is saved within Diplo*me*'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 utilizing 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 and independent way to verify that such data are the ones effectively saved within Diplo*me*'s ecosystem also in order to avoid man-in-the-middle issues. This is because being all data not openly accessible from verification a user or a third party may utilize external methods to modify the data while sharing.

Top layer (open to everybody but limited to entities with specific information) is therefore used to guarantee that anyone accessing directly the stored data can directly verify that the data as the following information are 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 are the same as the one's 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:

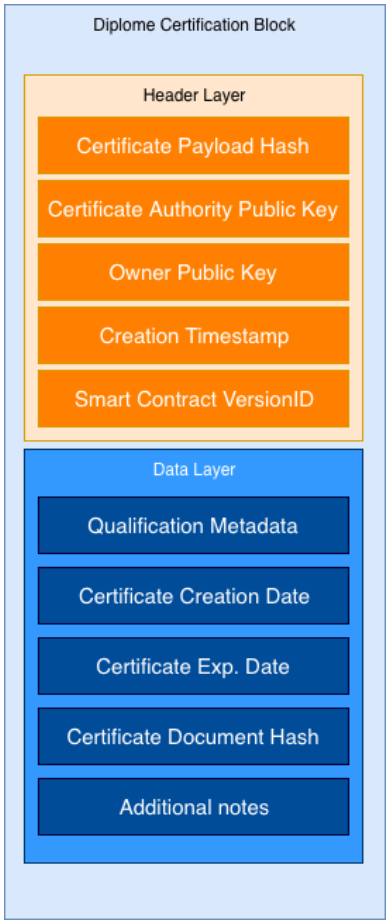


FIGURE 6 - LAYERED LOGICAL STRUCTURE

## Certification Process

Once an Organization (already part of Diplo*me*) decides to issue a new qualification certificate (or a copy) for a user, a complex process enforces and validates all required steps necessary to create a new metadata structure to be saved within user's wallet.

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

1. First it is encrypted with the private key of the issuing Certification Authority
2. Secondly, the resulting data is encrypted with the user's public key

In case the certification metadata is stored off-chain, the encryption will comprehend all the key referencing details of the off-chain location and content.

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

1. Decrypt the data with User's private key
2. Decrypt the resulting data with Certification's 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 contains implicitly the identification of the issuing CA
- In case a CA would loose 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 DOS attacks.

The previously described process is implemented and verified by Diplo*me*'s backend through Diplo*me*'s Smart Contracts.

The various Smart Contracts part of Diplo*me*'s solution have the duty to ensure that the previous process is duly followed and that all participants to the process are verified entities.

Entities willingly to issue a new certification are verified by the Smart Contract through a specific request to an external oracle handled by Diplo*me* 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 by the issuing Certificate Authority that from Diplo*me*'s point of view is responsible also for the protection of its private key used in certificate's issuing process. After 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 certificate must be issued by the same Certification Authority with an updated serial number. This information will be handled during the sharing verification process to guarantee that only the last version of the certificate will be issued by the users.

## Sharing Process

The process of certificate sharing can be performed in two different ways:

1. A secure and standardized way, sending the certificate via email to a destination entity together with full verification elements
2. As Verifiable Credential, e.g. issuing a signed credential fully compliant with W3C model

The standardized sharing model allows any receiving entity to securely and uniquely verify the issued certificate without any need of implementing new models and in case any need of deep technical knowledge: in fact a web-based verification service has been developed to have 1 step secure verification of the given data.

In case receiving entity will require the highest level of security in verification of the received certificate, a set of APIs have been developed at smart-contract level to enable direct verification.

The second sharing model aims to enable Diplo*me*'s ecosystem and its stakeholders and users to be in line with the latest models, standard and technologies.

In the process of sharing as Verifiable Credential, the *Holder* of the certificate (e.g. the owner of the Diplo*me* wallet where the certificate is stored) is allowed to publish to a third party (*Verifier*) a certificate provided by a Diplo*me* certified entity (*Issuer*) in a format compliant with the W3C standard ( Verifiable Credentials Implementation Guideline v1.0 ).

This allows the creation of a digital document that represents "*a tamper-evident credential that has authorship that can be cryptographically verified*" through the verification of the digital signature of the subject containing the claims that want to be shared with the document itself.

This enable the third party (*Verifier*) to autonomously access the content of the document and verify that it has been certified by a specific entity (*Issuer*) though a cross verification of such issuer that has been identified within the document itself through a **DID** (decentralized identifier document). The verifier can also check that "claims" stored within the document related to the "subject" have not been tampered with in comparison to the ones issued by the given issuer.

An example of a certificate shared as Verifiable Credential through Diplo*me* can be found below with a short description of the sections

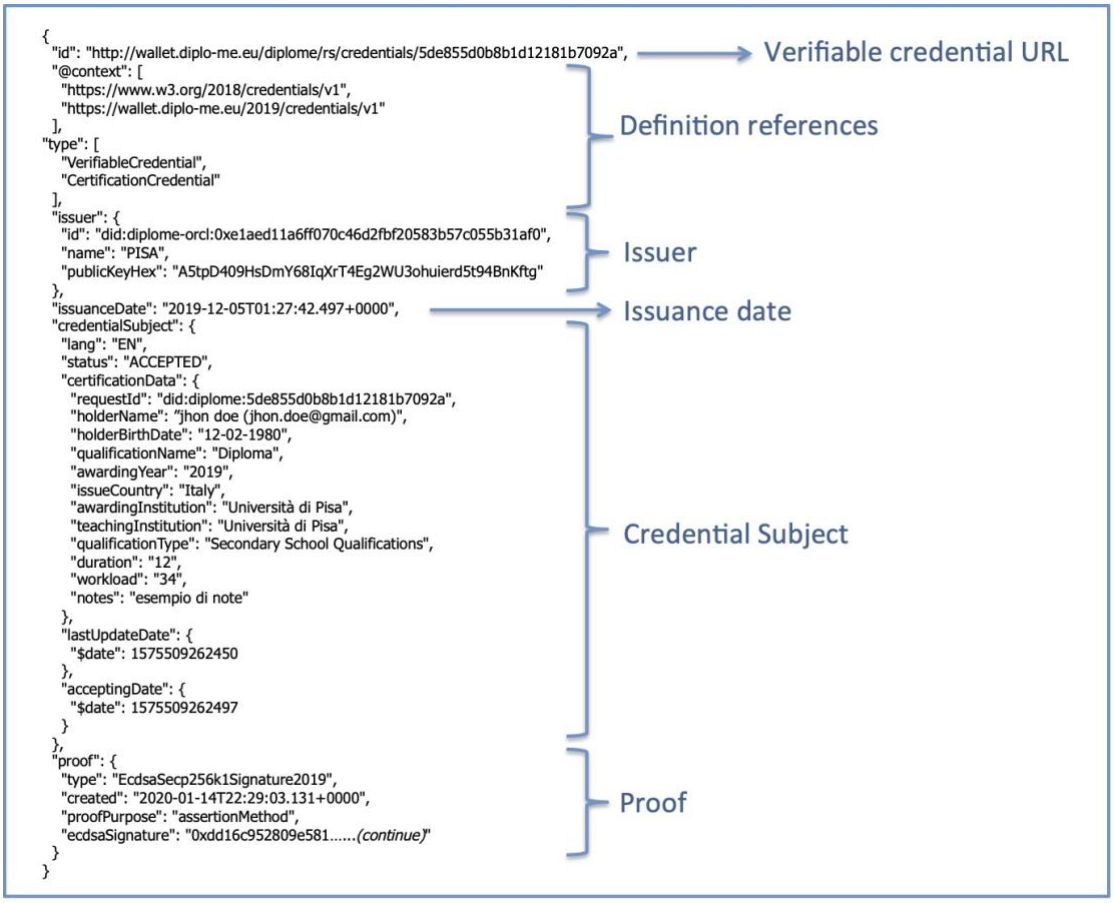


FIGURE 7 DIPLOME ISSUED VERIFIABLE CREDENTIAL

Let's understand in detail how this structure is built and can be used by a verifier:

1. Verifiable credential URL [W3C vc-data-model #Identifiers]
   It represents the universal identifier of the document in a Verifiable Credential format
2. Definition References
   It contains references to the definitions and context of the objects used within the digital document
   a. **@context** [W3C vc-data-model #context]: contains the URLs to the definitions of the objects references within the document
   b. **Types** [W3C vc-data-model #types]: lists the types of objects used within the document (and defined in the @context section)
3. Issuer [W3C vc-data-model #issuer]
   This section defines the issuing entity that created the credentials. The following elements are present:
   a. **Id**: the unique identifier of the issuer in DID format (decentralized identifier document) with the method ***diplome-orcl*** [W3C did-core #did-method] in reference to Diplo*me's oracle* that represent the source of truth in relation to the issuers.
   b. **Name**: issuer's name, used when registering with Diplo*me's* oracle

c. **publicKeyHex:** the public key of the issuer in HEX format

4. **Issuance Date** [W3C vc-data-model #issuanceDate]
   This attribute defines the date from which the credential must be considered valid, it could be equal to the issuing date of the certificate as an example.
5. **Credential Subject** [W3C vc-data-model #credentialSubject]
   This section contains all "claims" expressed by the issuer in relation to a subject. In our example it contains all metadata related to the issued certification.
6. **Proof** [W3C vc-data-model #proof]
   This section contains all information needed by the receiving entity (*Verifier*) to undertand the type of signature used to allow the secure verification of the issued claims that are stored into the CredentialSubject section. In Diplo*me's* implementation there can be two verification mechanisms:
   a. **External Proof**: it provides a JWT format (JSON Web Token) for signature generation and verification.
   b. **Embedded proof**: that provides a Linked Data Proof mechanism for data validation, e.g. based on a simple verification of the signature stored into the Proof section

At the moment Diplo*me's* choice have been to use the Embedded proof model: to generate the signature (**ecdsaSignature**) of the data contained into the **credentialSubject** structure, we selected the *EcdsaSecp256k1Signature2019* suite listed into the W3C document Linked Data Cryptographic Suites

## Data Privacy and Data Protection

### DATA PROTECTION PROFILES

Diplo*me* aims to be a worldwide solution the data protection approach is flexible in order to accommodate different legislations.

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

At the moment 3 data protection profiles are envisaged:

**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 Diplo*me* 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 user's blockchain account would be needed to complete the qualification certification process.

To give an example of a possible data structure following 'profile1'

```
"id": "http://wallet.diplo-me.eu/diplome/rs/credentials/5de855d0b8b1d12181b7092a",
"@context": [
  "https://www.w3.org/2018/credentials/v1",
  "https://wallet.diplo-me.eu/2019/credentials/v1"
],
"type": [
  "VerifiableCredential",
  "CertificationCredential"
],
"issuer": {
  "id": "did:diplome-orcl:0xe1aed11a6ff070c46d2fbf20583b57c055b31af0",
  "name": "PISA",
  "publicKeyHex": "A5tpD409HsDmY68IqXrT4Eg2WU3ohuierd5t94BnKftg"
},
"issuanceDate": "2019-12-05T01:27:42.497+0000",
"credentialSubject": {
  “certificationURL”:”https://ext.univ.com/certification/7ba66f76-a6fa-4d7c-8bc3-b4ee6dbbd123”,
  “certificationHash”: “18a4faa2331d46e4038a6ba25968f140857c106351ffab1579c4c678ec0f71e7”,
  “hashType: “Keccak-256”,
  “hashSalt”: “c596cab4607”
},
"proof": {
  "type": "EcdsaSecp256k1Signature2019",
  "created": "2020-01-14T22:29:03.131+0000",
  "proofPurpose": "assertionMethod",
  "ecdsaSignature": "0xdd16c952809e581……(continue)"
}
}
```


FIGURE 8 - VERIFIABLE CREDENTIAL ISSUED WITH PROFILE 1 DATA

The actual certification details are stored externally and lined with the “certificationURL”.

The integrity of this document can be verified through the “certificationHash” and “hashSalt” details.

**Profile 2**

The data structure representing the issued qualification is completely anonymized and protected with double encryption using the qualification organization key and user key. The full JSON representation of such qualification is stored within the blockchain user account. No identity data is stored within the qualification dataset.

**Profile 3**

The data structure representing the issued qualification is completely anonymized and protected with double encryption using the qualification organization key and user key. Identity data is stored into the wallet (e.g. SSI reference) together with the qualification representation in JSON format that includes full details of the qualification.

## DATA PROTECTION APPROACH

Regarding data protection, DIPLOME follows the PrivacyByDesign and PrivacyByArchitecture approaches.

At this purpose, to implement the appropriate rights management, the wallet created for a user at registration time is fully owned by the user itself, meaning that the data held by the wallet or related smart contracts within the blockchain network can be freely managed by their right owner for his own personal use as part of his willingness to have a certified and immutable copy of received qualification. Based on this design principle we can for example deduct that handling of such data fall under the household exemption of the GDPR.

As smart contracts are part of the Diplo*me* solution it is ensured that specific functions that can be called (executed) exclusively by the Certification Authorities and can be used for the good of the service provisioned.

Wallet’s public keys or addresses on a blockchain may be considered personal data: such address and keys are on full control of the user and the data stored into the related wallet and smart contracts unreadable without user’s explicit actions.

Diplo*me* cannot handle or modify any stored information even on 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 are the key metadata required to provide trusted information about the education 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 user's wallet and smart contract, all data related to any certified qualification is in full control of the user itself, and only he can give access rights to or disclose such data.

This allows as an example to give the user 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 user can "Reactivate" it restoring full functionality
2. Definitively 'canceling' the data through the "Destroy" function implemented into the smart contract: this function is not reversible and therefore user won't have 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 user's functions and data: in this way the user with all related contracts will be not accessible anymore and no reversibility will be possible.

### Openness and Portability

All data saved within user's account can be exported in standardized 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 to any modern IT system.

This design approach guarantees therefore full Right to Data Portability to DIPLOME users.

### Accountability

As per data accuracy section, data are linked uniquely and indissolubly to their source (Certification Authority). Full details on the specific event that created such data are also saved along (e.g timestamp, source details, etc).

Data access, based on 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 temper resistant (immutable) and any modification becomes impossible also 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 are 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 on several and structurally different attribute-values.

Diplo*me* aims to extend its capabilities with functionalities that will give access only to subset of the stored data giving therefore powerful tools to the end use to share only the information needed to perform the service he requires. For example he can share only the date of the issuing of the qualification or the final score.

## OWNERSHIP & COPYRIGHT



## STATEMENT OF CONFIDENTIALITY & NON-DISCLOSURE

This document contains proprietary and confidential information. All data submitted to the receiver is provided in reliance upon its consent not to use or disclose any information contained herein except in the context of its business dealings with Diplo*me*. The recipient of this document agrees to its content of its confidential nature.

The recipient agrees to instruct each member this document is disclosed to, that they must not disclose any information of this document to others except to the extent that such matter are generally known to and are available for use by, the public. The recipient also agrees not duplicate or distribute or permit others to duplicate or distribute any material contained herein without Diplo*me*'s express written consent.

Diplo*me* retains all title, ownership and intellectual property rights to the material contained herein including all supporting documentation, files, marketing material and multimedia.

By acceptance of this document, the recipient agrees to be bound by the aforementioned statement.