White Paper

RLDAC

January 2026

1 The problem

1.1 Document fraud

Fraud is a global issue: nowadays, anyone can commit fraud by forging any type of file in a few hours - or even minutes since AI tools became widely available. Hence, it becomes easier to bypass traditional controls and checks. Recognising this, we began considering ways to counter this tendency in a scalable and user-friendly way.

Fighting fraud by securing files and the information they contain has countless applications. We wanted to make sure we could provide a solution that gave a "complete" answer to combat fraud for a specific type of file. We found that written documents were a good starting point, and they constitutes the first set of use cases we tackle. For the future, we are working to expand our solution to different types of file (photos, videos, etc.) and specific contexts that come with their own set of constraints (supply chain, journalism, etc.).

Some solutions already exist: they go from automated Blockchain issuance processes, to more tailor made, or even manual systems, with all of them having pros and cons. Observing it nurtured the way we wanted our solution to look and feel like for institutions that need to protect their reputation and the value of the documents they issue.

1.2 Incomplete traditional solutions

If no proof mechanism is implemented in common document solutions, impersonation, data tampering, and data forging become serious risks .

To counteract this, traditional verification solutions generally rely on a long and tedious process, involving manual checks and back-and-forth communications for all parties involved. It results in delays, frictions, additional costs, and efforts for all involved. However, the underlying need remains the same: proving the credentials, diplomas, or supporting documents are authentic, and legacy systems do not address the problem systematically...

2 Our solution

2.1 The building blocks of our offer

We defined three necessary characteristics at the heart of our solution

- **Issuer authentication**, which consists in a proof that you issued a given document, and your identity cannot be forged
- **Data integrity**, meaning that the data you issue cannot be tampered with
- **Revocation**, to indicate that a specific credential is no more valid, or that it expired[1]

Our vision is to unite security and efficiency and offer the best of both worlds

- **Security** means that you can associate cryptographic proofs with the documents you issue, enabling third parties to verify them
- **Efficiency** means providing an all-in-one user-friendly solution to cover the whole document lifecycle

We consider the **Verifiable Credentials** framework as the optimal basis to design our solution.

[1] Credentials can also be temporarily suspended without being permanently revoked.

2.2 Verifiable Credentials in a nutshell

Verifiable Credentials[2] (VCs) are digitally signed credentials that let someone prove a set of claims (e.g. data contained in a document) in a way that is easy to verify and tamper-proof. They allow you to embed cryptographic proofs in the documents and credentials you issue, in order to

- **authenticate the issuer**
- **ensure data integrity**
- **revoke, suspend, or delete the credential** if necessary

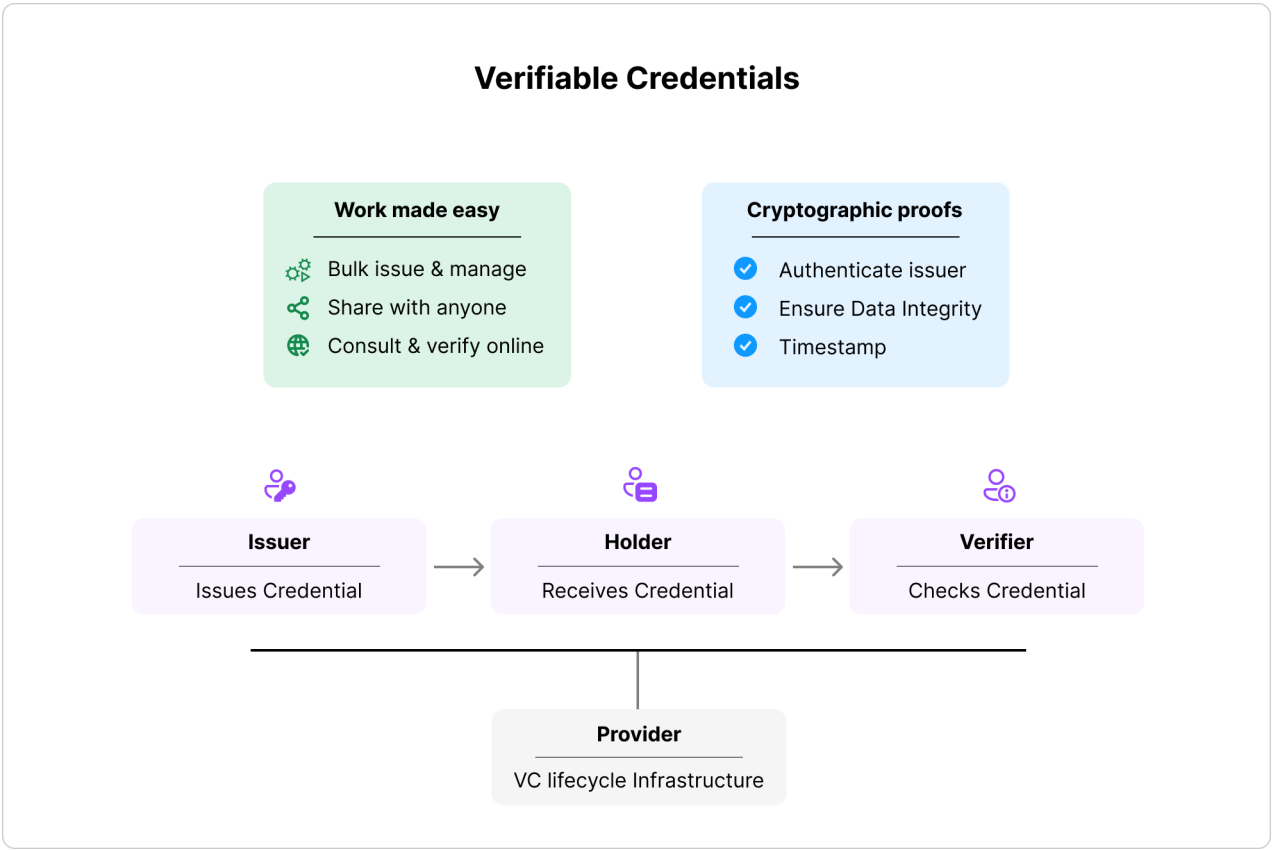
Their flexibility and interoperability make it easy to

- **display them** the way you decide
- **share them** with anyone
- **verify them** online

Interactions around a VC generally involve

- **an issuer** (or tenant) who creates it
- **a holder** (or recipient) who is designated by the VC
- **a verifier** who checks it when needed

A **service provider**, RLDAC for instance, can provide the infrastructure for issuance, verification, and revocation of the VCs.



[2]W3C VC 2.0 is the global standard for representing cryptographically verifiable credentials in machine-readable format. About W3C: https://www.w3.org/about/history

Compared with other systems - such as Blockchain for example - we found the off-chain VC to be the most efficient, secure, and environmentally friendly, in addition to being easily adaptable to data protection rules:

- Blockchain depends on the availability of a public network → VCs operate independently of third-party infrastructures, leaving credential issuance and lifecycle management under the issuer's control
- Blockchain requires publishing data or proofs on a shared ledger → off-chain VCs keep personal data outside shared infrastructures, enabling data minimization, selective disclosure, and compliance with data protection regulations
- Blockchain systems are not immune to unpredictable, high-impact events (fees bumps) → verifiable credentials do not rely on network fees or market-driven pricing, resulting in predictable and stable operational costs
- Blockchain is thought for being irreversible, and native revocation & suspension mechanisms are not in its nature → VCs natively include these mechanisms and permanent deletion is possible
- Blockchain can be energy intensive since it's a collective-decentralised system, and depending on its proof mechanism → VCs are much more efficient and only need single signing operations from the issuer, making it greener

2.3 Your all-in-one Verifiable Credentials Platform

Our solution gives you access to an all-in-one Platform to do everything you need about your Verifiable Credentials:

- **Connect** your data
- **Create & Manage** templates, groups, and campaigns
- **Issue & Manage** your VCs
- **Ease verification** by letting anyone check your VCs online
- **Monitor & Analyse** interactions around the VCs you issued
- **Revoke, suspend, reinstate, or delete** VCs when necessary

2.4 Data connection methods

2.4.1 Data ingestion

This data connection method has been thought for education credentials, as it gives a solution to the challenges faced by education institutions when they have to issue certificates and participate in background checks. Nevertheless, the process of data ingestion presented here can find its purpose for many other use cases.

Firstly, the industry of forged diplomas, made up of diploma mills and companies specialised in diploma forgery, has a global market size that increased from 300 million dollars in 2011 to 7 billion dollars in recent years[3]. It is a challenge for education institutions: the trust in them and in the diplomas or credentials they issue is at stake. Protecting institutional reputation becomes a strategic priority.

Secondly, beyond the initial gap between the completion of studies and the formal issuance of a diploma, graduates face recurring verification needs throughout their professional and academic lives. Employers, academic institutions, and other third parties regularly require trustworthy proof of qualifications. In order to complete these background checks, education institutions using traditional document solutions have to manually issue certificates and participate in endless administrative back-and-forth to confirm the information verifiers want to check.

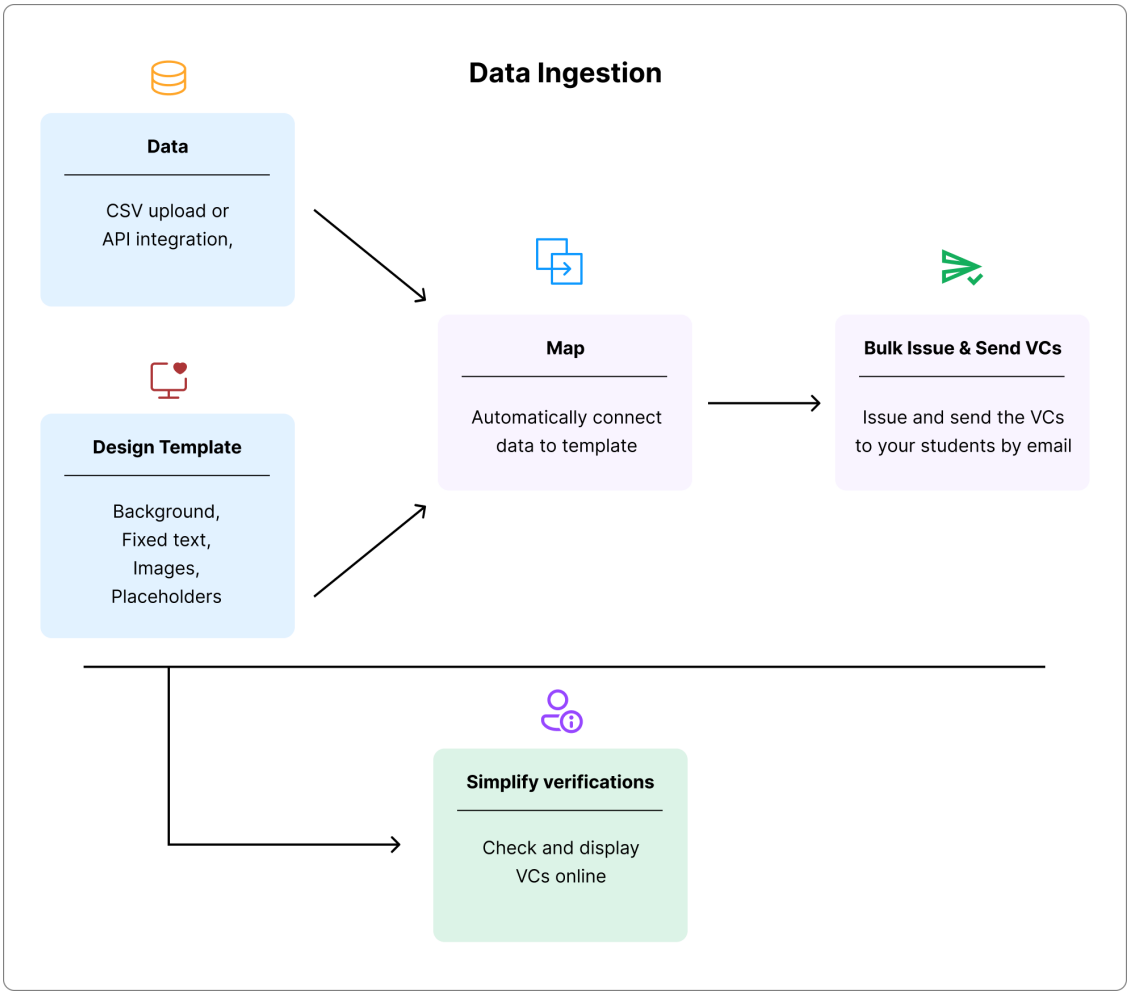
[3] `https://rm.coe.int/factsheet-countering-education-fraud/1680b1c5f9`

With our solution, you can benefit from a faster and automated process to generate branded and personalized credentials at scale:

- **Load your data** on the Platform by uploading a CSV or by API integration
- **Design your templates**, brand them, and benefit from a new communication channel
- **Map the fields** between your data and your template
- **Bulk-issue VCs** displaying your design and your student's achievements
- **Send the VCs** and their associated links in bulk by email to students[4]
- **Ease verifications** by allowing your students to share the VC they own - or its link - enabling third parties to conduct online verifications by themselves

Once you upload your data and connect it to a template[5], the whole process of bulk issuance and sending of the Verifiable Credentials and their links is done in a few clicks, saving you the time and efforts of creating and transferring each credential one by one manually.

Thanks to the proofs embedded in the Verifiable Credentials, all the subsequent verifications are done online and fully automated. This way, verifiers do not need to contact you when they perform background checks



[4] You can also use the API to directly offer the credentials for download on your domain

[5] After the CSV is uploaded, a mapping interface will be provided to map CSV columns to VC claims. This interface will allow the issuer to associate each column in the CSV with the corresponding field in the VC schema, ensuring that data is accurately represented in the issued credentials.

2.4.2 Data extraction

This data connection method has been thought for supporting documents, as it gives a solution to the challenges faced by supporting documents issuers (banks, insurers, energy and telecom providers, employers etc.) to prevent fraud, protecting their reputation and their clients.

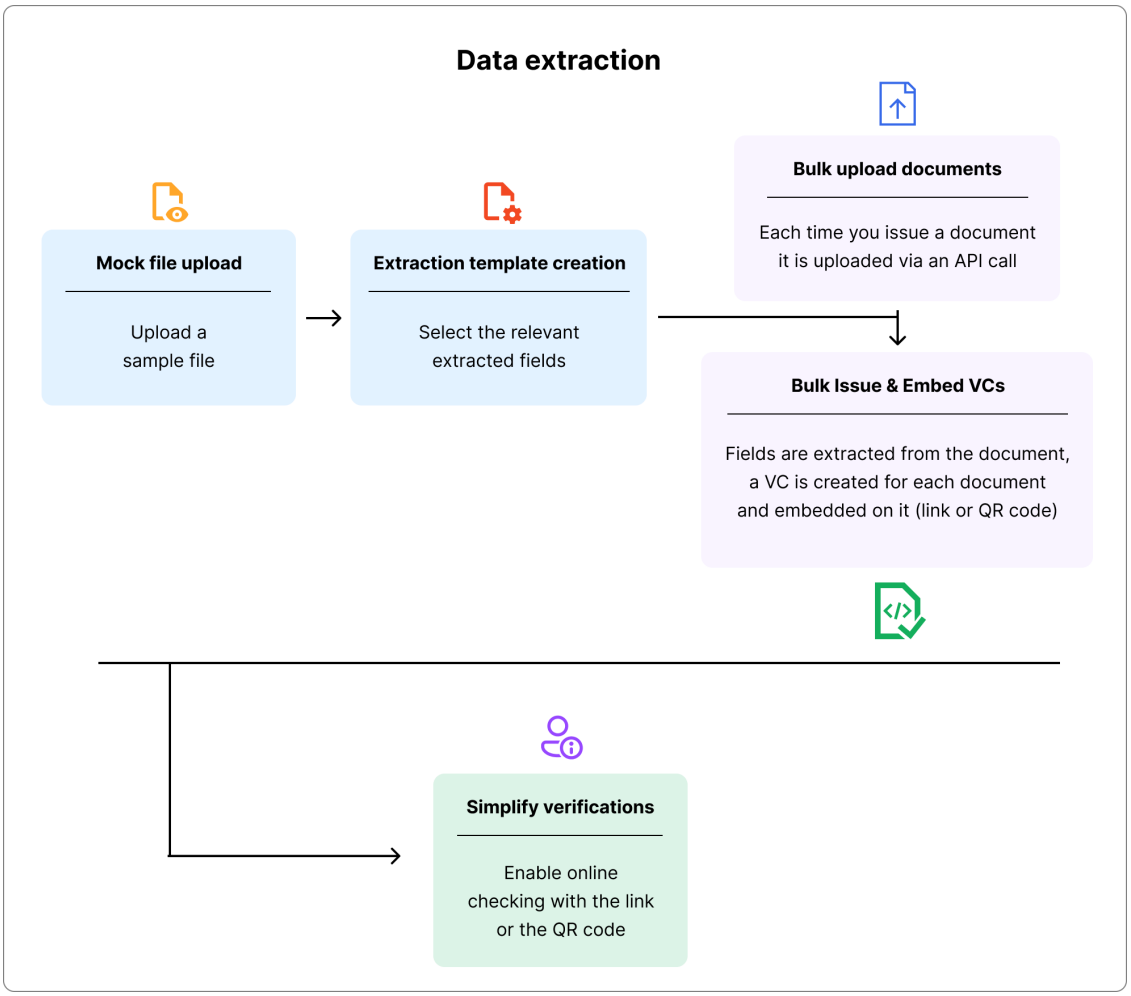
Ensuring supporting document's integrity is paramount to fight fraud in general. It ranges from performing background checks (for loan or job applications) to protecting the reputation of the institutions issuing supporting documents and their clients (identity theft, targeted fraud, etc.).

Thanks to the data extraction method, supporting document issuers can integrate bulk Verifiable Credential issuance into their existing process by completing the following steps on the All-in-one Platform:

- **Upload example**: Share a sample document, ideally a template
- **Create the extraction template**: we generate an extraction template for the verification-relevant fields, you can review and fine-tune it
- **Issue automatically**: for each document you produce, we extract the fields from it and create a VC containing a timestamp and your signature to ensure data integrity
- **Embed VC**: with an API call, you can automatically add the VC link or QR code onto the supporting document you issue every time a user requests/downloads the document
- **Ease verifications**: anyone can then verify the supporting document online by using the link or the QR code

For every document you issue, we embed a link or QR code that corresponds to a timestamped Verifiable Credential, signed by you, and cryptographically bound to the data you put in the document.

Once your extraction template is set, issuance and verification are automated: no extra steps for your teams, and third parties can verify the authenticity and integrity in seconds.



2.5 Deployment modes

To deploy our Solution, you have the choice between two modes:

- SaaS - Delegated mode: we take care of all the Verifiable Credentials lifecycle, from issuing the VC, to hosting the data to display them and complete the verification through our servers
- On-prem - Local mode: you take care of all the Verifiable Credential lifecycle, installing the Solution on your servers and updating it when we release new versions or patches

2.6 White-Label

The On-prem - Local mode is *de facto* fully White-Label.
In the SaaS - Delegated mode, you can choose a fully White-Label plan, hosting on your domain the verification page we provide, and sending the emails from your domain name if you use the data ingestion method.

2.7 Governance and Compliance

2.7.1 Zero-Trust model

A central principle of the SaaS Platform is its Zero-Trust design (the On-Prem Platform is already Zero-Trust by nature): the Provider must never be in a position to forge credentials, impersonate an issuer, or modify any credential's content or status without detection.

This is achieved through strict separation of responsibilities, cryptographic guarantees, and verifiable auditability.

In order to conduct audits of this zero-trust model, an Open Source Audit Kit is provided to every issuer. For example, every signing operation is logged by the issuer's system, ensuring tamper-evident traceability. As a consequence, the Provider:

- **Cannot forge a credential** on behalf of an issuer
- **Cannot alter a credential's content**, because any modification would invalidate the cryptographic signature
- **Cannot serve forged metadata or forged validity result** on the verifying webpage

2.7.2 GDPR

The Provider acts as a data processor for the Issuer who is the data controller and who should therefore determine a legal basis for processing personal data.

The revocation mechanism, native to the W3C VC2.0 framework, and the possibility to permanently delete Verifiable Credentials as they do not require on-chain storage, enable to be fully compliant with the right to be forgotten, as stated by the GDPR.

3 Legal mentions

RLDAC
SAS, société par actions simplifiée
6 RUE D'ARMAILLE, 75017 PARIS, FRANCE
SIREN: 999398480
VAT: FR45999398480