Technical Information on the M-Cred Platform

Version 1.0

May 2026

The up-to-date edition of this documentation is published at:
https://docs.m-cred.com

m.cred.com | info@m-cred.com

Table of Contents:

General Information: Introduction to Managed Credentials with M-Cred

As a business aiming to advance academic administration, **M-Cred** is an entrepreneurial initiative financially supported by Gebert Rüf Foundation and several universities in Switzerland.

As a product, **M-Cred** is a modern and highly capable platform to issue digital micro-credentials in schools, in higher education, and in training/qualification scenarios. These credentials are portable and verifiable, and accurately describe the learning objectives and competences by the recipients. The platform is internally operated through various roles without direct access by recipients, who rather receive links to the delivery of credentials. The outstanding features of the platform are:

- Digital souvereignty: Institutions decide themselves if they want to self-host or use a provisioned service (SaaS). **M-Cred** is entirely based on open source software and not subject to usage restrictions.
- Digital inclusion: **M-Cred** produces digital credentials in various formats (artefacts) including PDFs which can be printed. That makes the credentials inclusive and gives a connecting element between the physical and digital worlds. Hence, the introduction of micro-credentials can be gradual while acceptance of Open Badges and other format grows.
- Digital leadership: **M-Cred** integrates with leading student and course management systems (Evento, IS-A and others) as well as with secure mobile phone wallets (Swiyu/e-ID, EUDI + PKPASS). Further trust infrastructures and verifiable credentials (VCs) in other countries can be added.

Through its country catalogues and support for competence catalogues such as European Skills, Competences and Occupations (ESCO), as well as internationalised user experience, setting up scenarios and pilots with **M-Cred** is possible in short time for all universities and countries.

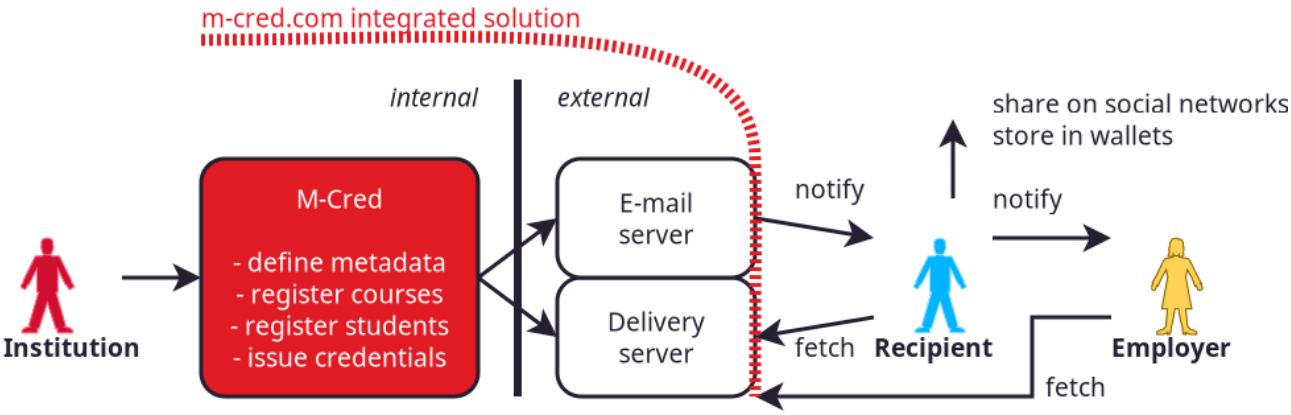
The technical characteristics are a strong motivation to use **M-Cred** for the issuance of achievement proofs. This document explains the technical perspective so that decision makers can get a full picture of the platform's capabilities.

It should be noted that a pilot and rollout often comes with a lot of coordination on legal topics, design, communication, and administrative work on ensuring high-quality course descriptions. The **M-Cred** team is experienced in facilitating these discussions and explaining the possibilities.

Platform Workflows

The platform has its place in the general workflow of verified credentials involving an issuer (institution such as university or government, using M-Cred), a recipient (e.g. student), and a verifier (e.g. future employer).

Credentials are delivered to recipients with an e-mail containing a link to a delivery server, essentially a hardened web server. The recipients then decide about forwarding these links to employers or for other purposes, such as additional studies, and managing and sharing the credentials as they like.



Institutions decide whether to use the integrated servers (e-mail and delivery) from m-cred.com as white-labelling solution, or whether to use other servers for this purpose. For example, a university may use a government-provided e-mail server and an NREN-provided delivery server. The M-Cred team will then set up the integration accordingly.

In any case, neither recipients nor employers need direct access to the M-Cred platform, which remains an internal tool.

Platform Infrastructure Information

M-Cred is offering the following two infrastructure flavours for rolling out micro-credentials in production: self-hosted and centrally hosted. The choice between the flavours depends on strategic and financial decisions by the operators.

- Self-hosted on issuer premises. This is the recommended option for larger-scale deployments and ensures that all data remains in the respective country of the issuer. It requires a dedicated contract.
  - contact the M-Cred team if interested to learn about conditions and technical requirements
  - e.g. university servers with university domain names in any country such as **issuance.university.edu** (internal issuance running M-Cred platform) and **badges.university.edu** (public access to recipients)
  - servers hosted by the government or by the respective NREN (national research and education network) for multiple educational institutions - as M-Cred is multi-tenant capable, this scales up easily to hundreds of tenants

- Centrally hosted production instance on the issuance server **https://management.m-cred.com** with valid contract. This is the always-available option where accounts can be set up after a contract has been signed.
  - may have external domain name aliases and custom e-mail accounts to be used as white-labelling solution
  - highly secure setup with network-level access restrictions, encrypted disk, backup, monitoring etc.
  - no access by recipients/students to the issuance system, only by qualified staff
  - full integration with e-mail notifications and delivery of credentials to the rightful recipients at the public server **https://credentials.m-cred.com** along with long-term secure storage

Furthermore, two additional flavours are available for non-production use cases and for exploring the capabilities of the system in pilots and demonstrations:

- Development version at **https://dev.m-cred.com**

    - possibility to follow the latest development or try out custom functionality
    - accounts are created on demand by the M-Cred team, e.g. for pilots, even before signing of contracts
    - safety: no e-mailing of credentials, instead the mailbox is made available for inspection
    - delivery of credentials to the exemplary recipients on the same server (**https://dev.m-cred.com/mcs/**), with short validity to prevent mis-use

- Public demo account at **https://demo.m-cred.com**
    - login with public demo users (access defined on other page) to experience the credentials issuance process of the exemplary Testikon University
    - safety: fixed accounts which are reset every full hour
    - safety: no e-mailing of credentials
    - delivery of exemplary credentials on the same server, with short validity (**https://demo.m-cred.com/mcs/**)

All **m-cred.com** infrastructure is hosted in Switzerland and complies with the relevant regulations concerning security and data protection. It is the responsibility of the M-Cred team to protect the data. The data protection contact is **info@m-cred.com**.

For self-hosted instances, the regulations of the respective country apply, and the responsibility is with the respective local operator.

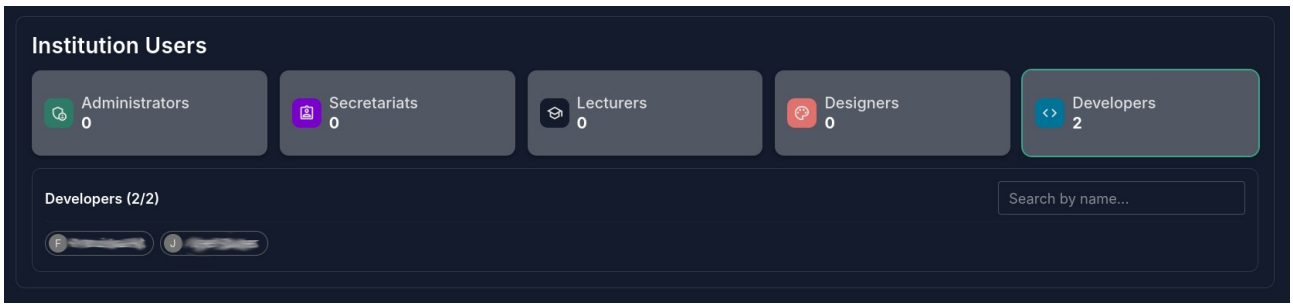
Platform Roles

The issuance of micro-credentials with M-Cred is governed through well-defined roles per institutions. The roles are:

- Admin. An administration person in an institution who defines the metadata and important policies, such as which MC formats to issue or which student attributes to capture, as well as wallet integrations.
- Designer. A designer defines the visual appearance of MC-related documents. This includes, depending on the artefact configuration by the admin, the Open Badge PNG, the badge web rendering in HTML, the confirmation PDF, and the e-mail messages to recipients and to the institution.
- Secretariat. In this role, courses/modules and classes with students are administered. This encompasses the definition of competences and the learning-related metadata that complements the institutional metadata to define the content of credentials.
- Lecturer: The first task of a lecturer is to propose courses/modules to the secretariat, specifying the learning objectives and other crucial information that requires domain knowledge. The second task of a lecturer or course-responsible person is to assess whether a person becomes a rightful recipient of a credential or not, with pass-fail or grade decision depending on the grading scheme defined by the secretariat.
- Developer, combining the scopes of the other roles. This role only exists on the dev/demo instances to allow for full exploration without having to switch roles.

Moreover, the assigned institutions are also defines as a special role, so that each natural person will have as a minimum always two roles.

When logging into M-Cred, the dashboard shows statistics about all roles per institution.



Platform Schemas

The production of credentials is governed by the norms, regulations and conventions that exist in the institution's country. For instance, in Switzerland, MCs are defined to be 1-9 ECTS whereas skills badges carry 0 ECTS, and in case grading is used, 6 is the best grade and 4 is the passing grade. The existence and refinement of schemas in the country catalogue simplifies institutions in getting started with legally valid and recognised credentialling.

At present, the following countries are available from the country catalogue:

	Austria (AT)		Ireland (IE)
	Brazil (BR)		Republic of Korea (KR)
	Switzerland (CH)		Türkiye (TR)
	Spain (ES)		Ukraine (UA)
	Finland (FI)		Pakistan (PK)

The M-Cred team works with universities and government agencies to ensure that all relevant information is accurately reflected in the country catalogue.

An online view of the country catalogue is available here:
https://docs.m-cred.com/ccbrowser

Additional schemas govern the available MC formats, wallet integrations, student attributes along with import from heterogeneous sources, and educational settings/terminology.

Platform Accounts (Non-Production)

Accounts for the publicly accessible system demonstration at **https://demo.m-cred.com**, referring to the ficticious Testikon University (TU-Demo) located somewhere in the Swiss mountains:

User name	Password	Explanation
`demo`	`Demo24/7`	developer view, i.e. all functionality
`demo-maint`	`Demo24/7`	admin/design maintenance, i.e. no students or courses

Accounts for **https://dev.m-cred.com** and for the production instances:

All accounts are assigned a combination of role and institution.

- Institutions: TU (for miscellaneous testing), and others
- Roles: admin, designer, lecturer, secretariat, developer

All accounts for the developer instance are administered through **https://devauth.m-cred.com**. There are generic accounts not bound to any person (e.g. lecturer@tu), but also personalised accounts with actual names and e-mail addresses.

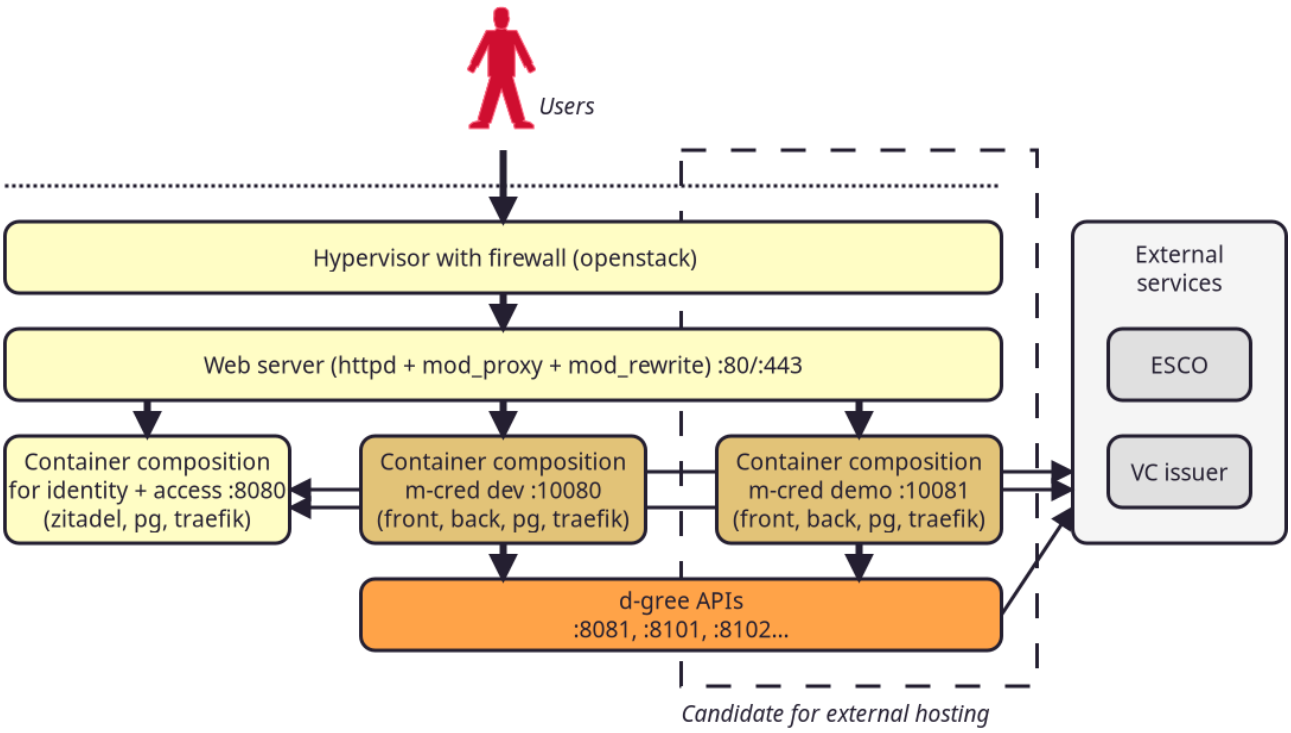
Accounts for the production instances are administered separately.

Platform Architecture and Infrastructure Topology

On the surface, M-Cred consists of a web-based user interface to which access is granted through an authentication service (Zitadel) depending on the roles configered by it. Beneath the surface, the platform also runs a backend API, a relational database, several routing/proxy components, and integration with internal and external services. Internal services are operated potentially on the same physical machine but in privilege-separated accounts, such as the d-gree API to run the artefact preview and generation processes for credentials.

The two non-production dev/demo instances share a physical system but are differentiated by the stack versions and databases. The centrally hosted production flavour follows a similar topology but is physically separated, as are self-hosted instances.

The technology stack is operated by a container composition which is generated from templates for a specific flavour. Web access is typically proxied through secured subdomains, such as **https://dev.m-cred.com** referring to the development instance of M-Cred through appropriate rules in Apache and Traefik.



Primarily, the internal d-gree APIs are used. They are defined in the following table. All of them require the 'institution_profiles' directory to be present as shared data layer.

Depending on the chosen artefact formats and wallet integrations, further internal services are used on demand. Currently, these internal services are shared among all M-Cred flavours, and accessible for users through the corresponding buttons in the web user interface.

API	**Invocation**	**Notes**
MC production	:8081/?contentlang=<lang>&inst=<inst>&issuedate=<date>&sub=<students>&artefacts=<artefacts>&api=true[&apiref=<apiref>]	container permanently running; returns workspace id for progress tracking on :8081/progress?workspace=<workspace>; artefacts=auto; apiref=ref/test; inst=Inst/Inst-Course
Badge image rendering	:8101/renderbadge/<inst>/<course>	container started on demand; returns PNG
Document template rendering	:8101/renderdoc/<inst>/<course>	returns PDF with placeholders
Template validation	:8102/validate/<inst>/<course>	no container, very fast response
Backup and data export	:16050/dataportability/<inst>	returns ZIP file with database contents including anonymised personal data

External services: ESCO is used in the frontend when defining skills and competences through the ESCO catalogue instead of bullet point lists with plain text.

Moreover, external services can be integrated as follows in the backend configuration.

- E-Mail: SMTP or Office 365 Graph API.
- LinkedIn: Native integration.
- VCs: As part of the artefact generation process, VCs are issed through configured systems such as Swiyu or Heidi Universe.

M-CRED

Platform Technology and Interoperability Information

M-Cred is based entirely on open source technologies to reduce vendor lock-in and strengthen the digital souvereignty perspective for administrations. The key technologies are explained here.

ZITADEL

Zitadel is used for identity and access management.

https://zitadel.com/

d-gree

D-gree is used to produce micro-credential artefacts.

http://d-gree.org/

PostgreSQL is used to store all configuration master data.

https://postgresql.org/

docker

Docker is used for running containerised workloads.

https://docker.com/

podman

Podman is used for unprivileged container workloads.

https://podman.io/

APACHE HTTP SERVER PROJECT

Apache httpd is used as primary web server and proxy.

https://apache.org/

Moreover, M-Cred integrates with a number of other systems, the selection of which depends on the chosen deployment flavour:

- e-mail delivery
- verified credentials (VC) issuance, such as Swiyu and Heidi Universe
- student and course management systems, such as Evento and IS-A
- social networks, such as LinkedIn

In terms of long-term verification of credentialling artefacts, M-Cred adheres to the relevant standards:

- Open Badge version 2 (hosted and signed);
- PDF and PDF/A.

This ensures interoperability, for instance with the many existing Open Badge validators.