Certify

GUIDE

GUIDE FOR BUYERS AND PROCUREMENT TEAMS

Choosing a digital credential platform: a buyer's guide

Most platforms look alike in a demo. The differences that matter show up later: in the recipient's experience, in what the price actually covers, and in what happens to your badges if you leave. This guide helps you find them before you sign.

By **Rob Tyler, Co-founder, Certify** · Updated 26 September 2026 · 8 min read

Online version: https://www.certify.one/guides/choosing-a-digital-credential-platform

THE SHORT ANSWER

Shortlist platforms on five things: open standards, the recipient's experience, integrations with the systems you already use, data protection, and exit terms. Then compare prices on a like-for-like basis using your own expected volumes, and test the claim and share steps yourself on a phone before you decide.

What does a digital credential platform actually do?

A digital credential platform lets you design badges and certificates, issue them to learners, deliver them, host a verification page for each one, and help recipients share them. Most also report on how badges are used and connect to learning systems so issuing can happen automatically.

In practice, you are buying six capabilities:

Capability	What it covers
Design	Badge and certificate templates, branding, criteria and metadata
Issue	Manual, bulk upload, automatic from an LMS or event system, or through an API
Deliver	Notification emails, and sometimes other channels
Verify	A public page for each credential that anyone can check
Share	Adding to LinkedIn, downloading, embedding and sharing links

Capability	What it covers
Manage and report	Expiry, revocation, corrections, analytics and user roles

Before you speak to any vendor, write down which of these you need at launch and which can wait. It stops the demo from setting your requirements for you.

Which features are must-haves?

Five areas separate platforms that work well for years from ones that cause problems: standards, recipient experience, integrations, credential management and data protection. Get these right and most other features are a matter of preference.

Open standards. Credentials should be issued to the Open Badges (https://www.1edtech.org/standards/open-badges) standard maintained by 1EdTech, so they can be read by other systems and don't depend on one vendor. Ask which version of the standard the platform issues to, and whether its implementation has been certified by 1EdTech.

Recipient experience. Ask to receive a test badge yourself. Check how many steps it takes to see and share it, whether an account or password is required, and how it looks on a phone. This is where claim and share rates are won or lost.

Integrations. List the systems you will issue from, such as your LMS, CRM, event platform or HR system, and ask how each connection works. A native integration, a no-code connector and "use our API" are very different amounts of work for your team.

Credential management. You will need to correct mistakes, reissue, set expiry dates and revoke credentials. Ask to see each of these in the demo, and ask what the verification page shows afterwards.

Data protection and security. Ask where data is stored, which sub-processors are used, what a data processing agreement looks like, and what independent evidence of security the vendor holds.

What should you ask about data protection and security?

Ask where recipients' data is stored and processed, who else handles it, and what evidence the vendor can show of its security controls. As the issuer, you are usually the controller of learners' personal data under UK GDPR, and the platform is your processor, so you need to be satisfied with how it handles that data.

Questions to put in writing:

- Where is data stored and processed, and are there any transfers outside the UK or EEA?
- Which sub-processors does the platform use, and how are you told about changes?
- Will the vendor sign a data processing agreement on terms your organisation accepts?

- What information appears on a public verification page, and can recipients control it?
- How does the platform handle a recipient's request to have their data deleted?
- What independent security certifications or assessments does the vendor hold? Ask to see the certificate itself, including its scope and expiry, rather than relying on a logo on a website.

The ICO's UK GDPR guidance (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/) is the reference point for your own obligations as controller.

How do digital badge platforms price, and how do you compare them?

Platforms charge in several ways: per credential issued, per recipient, by annual tier, or by a base fee plus add-ons. Headline prices are rarely comparable, so model the cost for your own volumes over three years rather than comparing list prices.

Questions that expose the real cost:

- What counts as one credential? Is a reissue, correction or renewal charged again?
- Are features you need, such as your own branding, integrations, analytics or single sign-on, included or sold as add-ons?
- What happens if you issue more than your tier allows in one year?
- Are there set-up, onboarding or support fees?
- How much does the price rise at renewal, and is that written into the contract?

Build a simple model with your expected issuance in year one, year two and year three, including renewals and reissues, and ask each vendor to price it. The differences are often larger than the list prices suggest.

What happens to your badges if you leave a platform?

This is the question most buyers forget to ask, and the one that matters most in the long run. Learners will keep your badges on their profiles for years. If verification links stop working when your contract ends, every one of those badges stops being verifiable.

Ask each vendor, and get the answer in the contract:

- Do verification pages stay live after the contract ends, and for how long?
- Can you export all credential data, including recipients, criteria and issue dates, in a usable format?
- Are credentials issued to an open standard, so another platform could recognise them?
- Is there a fee for exporting or for keeping credentials verifiable after you leave?

How does buying work for UK public sector organisations?

Public bodies buy under the Procurement Act 2023 (https://www.legislation.gov.uk/ukpga/2023/54/contents), which came into force on 24 February 2025, and often through frameworks such as G-Cloud, run by the Crown Commercial Service for cloud software. Which route applies depends on your organisation and the contract value, so involve your procurement team early.

Things that commonly come up in public sector buying:

- **Route to market.** Ask whether the vendor is on any framework your organisation uses. If not, your procurement team will advise on the right process for the contract value.
- **Data protection impact assessment.** Many public bodies will want a DPIA before issuing credentials that include personal data. Ask the vendor for the information you need to complete it.
- **Cyber security.** Many UK government contracts that involve handling personal data require Cyber Essentials certification, and some require more. Check your own requirements.
- **Accessibility.** Public sector websites and apps must meet the accessibility regulations, which point to WCAG 2.2 at level AA. Ask how the platform's verification pages and recipient screens meet that standard.
- **Social value and local suppliers.** Some public buyers weight these in their evaluation, so it is worth asking vendors for relevant information.

What should you ask in a demo?

Ask to see the parts of the platform you will use every week, not only the ones that look good. Bring your own badge, your own learner list and your own use case, and ask the vendor to show you each step with them.

1. Issue a badge to me now, and let me claim and share it on my phone.
2. Show me a bulk issuance to 500 learners, including what happens with a wrong email address.
3. Show me how issuing works from our LMS, step by step.
4. Correct a spelling mistake in a recipient's name. What does the verification page show afterwards?
5. Set an expiry date and show me the renewal flow.
6. Revoke a credential. What does someone checking it see?
7. Show me the analytics a programme owner would use each month.
8. Show me how our branding appears on the badge, the email and the verification page.
9. What happens to our credentials if we leave?
10. Walk me through your data processing agreement and sub-processor list.

How should you score the platforms on your shortlist?

Agree the weightings before you see any demos, then score each platform against the same criteria. That protects the decision from whichever vendor gave the most polished presentation.

Criterion	Suggested weight	What good looks like
Recipient experience	20%	Few steps to claim and share, works well on mobile
Integrations	20%	Works with your LMS and other key systems without custom work
Standards and portability	15%	Open Badges, clear export and post-contract verification
Data protection and security	15%	Clear data location, acceptable DPA, independent evidence
Credential management	10%	Corrections, reissue, expiry and revocation handled cleanly
Reporting	10%	Claim, share and verification data you can act on
Three-year cost	10%	Transparent pricing for your modelled volumes

Adjust the weights to your goals. A compliance-driven programme might weight credential management higher; a marketing-driven one might weight recipient experience and reporting higher.

CERTIFY ACADEMY

Learn it in Certify Academy

If you are new to digital credentials, the free Digital Badge Practitioner pathway is a quick way to learn the terms vendors use. Module 1 explains Open Badges and verifiable credentials, and Module 3 covers issuing workflows and measurement.

Learn the basics first, free → (https://academy.certify.one/en/pathways/digital-badge-practitioner)

Frequently asked questions

What is the difference between a digital badge platform and an LMS?

An LMS delivers and tracks learning: courses, enrolments, progress and completion. A digital badge platform recognises that learning with verifiable credentials that learners can share and others can check. Many organisations use both, with the LMS triggering badge issuance automatically when a learner completes a course.

Do we need Open Badges compliance?

For most organisations, yes. The Open Badges standard means your credentials carry their data in an open format that other systems can read, so they are not locked to one vendor. Ask which version a platform supports and whether its implementation is certified by 1EdTech.

How long does it take to launch on a new platform?

A simple launch with a few badges and manual or bulk issuing can take a few weeks. Launches that depend on integrations with an LMS or other systems, internal approvals, or a public sector procurement process take longer. Ask vendors for a realistic plan based on your requirements, not a best case.

Can we move our existing badges to a new platform?

Sometimes, but it depends on the old platform. Check whether you can export all credential data, whether old verification links will keep working, and whether the new platform can import or reissue credentials. Asking these questions before you sign with any vendor avoids the problem next time.