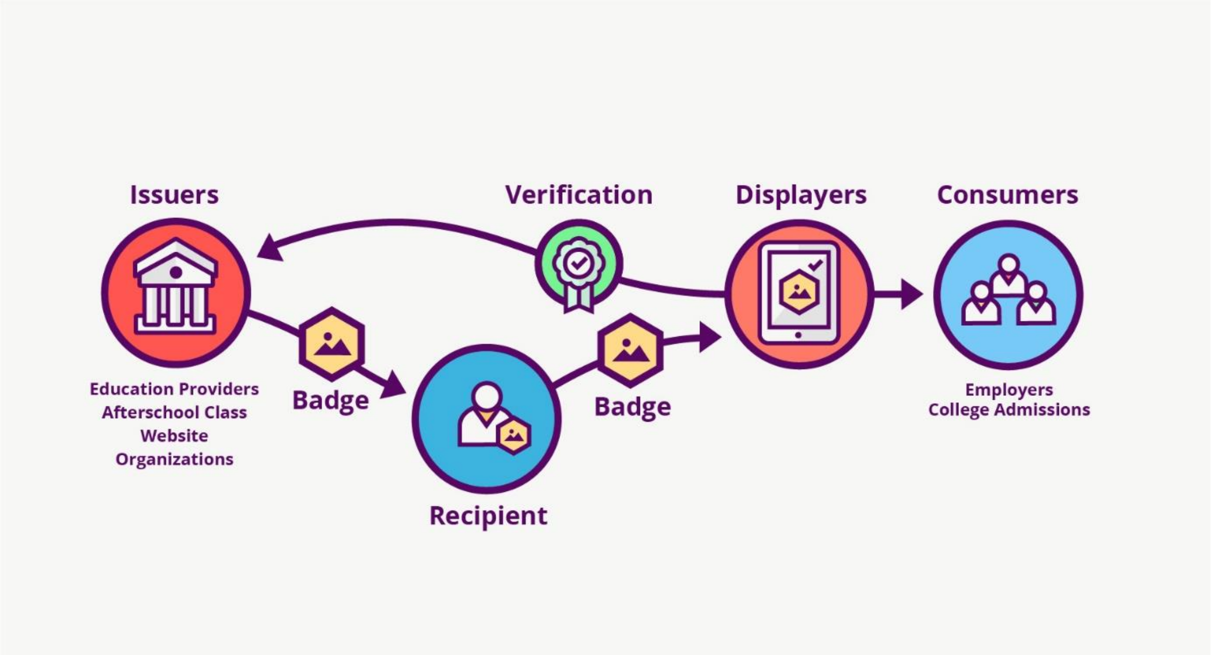
Open Badges

Issuing Open Badges **requires constructing and publishing a set of interconnected resources** that follow the structure and guidelines set out in the Open Badges Specification. The properties that make up a badge's metadata are split across these resources depending on where they apply. Together they form an Open Badge. For each badge awarded, there's:

- **An Issuer Profile** describing the individual or organization awarding badges. The information in the profile will appear in the **metadata for all badges, including name, description, contact email address, and website URI.** One Issuer profile is typically shared between all the badges an organization awards, though Issuers may choose to operate several Issuer profiles in order to serve specific audiences better. For example, a complex issuing organization like a university may choose to allow individual departments or staff to define their own issuing profiles so badges appear as awarded by a specific program or professor.

- **A BadgeClass,** the formal description of a single achievement the Issuer recognizes. This includes information such as **the name, description,** and of course the **graphic image (PNG or SVG)** that's the visual face of the badge, but also links to detailed criteria for how the badge may be earned and the Issuer profile that created it. A human readable criteria page and an image file visually symbolizing the accomplishment must be published at a stable URLs. Optionally, badges may be organized by tags or alignments to educational standards, and if included, that information appears in the BadgeClass.

- **An Assertion,** the record of an individual's achievement of the badge. The Assertion **links to one BadgeClass** and contains the information specific to one Recipient's achievement of the badge's criteria, **like the date it was awarded**, **the encoded Recipient identifier** it was awarded to, and optionally a **link to evidence** and an **expiration date**. An Assertion is the entry point for badge verification, and it may be delivered either as a hosted object with an accessible URL alongside the BadgeClass and Issuer profile resources, or as a cryptographically signed document given to the Recipient in order to distribute to relevant Consumers. **A single BadgeClass may be awarded to many different individuals by creating an Assertion for each Recipient**. A single Open Badge (sometimes called a "badge instance") consists of a unique set of one each of an Issuer, BadgeClass and an Assertion, though the Issuer and BadgeClass are often shared across many Badge Instances. When each resource has been created, the Assertion may be "baked" into a copy of the badge image, and the badge may be delivered to the Recipient and stored anywhere that can keep image files. Open Badges are typically **stored in Recipients' accounts at Open Badges backpack services**, from which Recipients may share them with Consumers whenever the verifiable badges are relevant.



A Typical Issuing Scenario

Several staffers at an after-school club get together. They want to recognize learning that's happening in their program with Open Badges. They:

- Set some general goals they hope to accomplish using badges to guide their design decisions.
- Decide to recognize a specific skill with a particular badge and come to agreement on how they will embed issuing this badge into their day-to-day practices.
- Design the badge and define the badge metadata in their Open Badges Issuer application.
- Publish the Issuer Profile and BadgeClass, start assessing students' achievement, and awarding the badge to individual Recipients.
- Send the awarded badges to Recipients by email, following the instructions in the program's chosen issuing software
- Other system designs for programs offering badges may involve students applying for badges by submitting evidence and program staff reviewing applications. Badge systems may integrate with online learning environments and award some badges automatically as a result of interactions that meet defined criteria. But, however badge systems are designed, if the Issuer uses Open Badges, students can combine the badges they've earned into collections together with all the Open Badges they've earned in other parts of their lifelong learning journeys.

Issuing Requirements

Issuer organizations may use one of the **available issuing platforms or establish their own Issuer service** by running open source code or building their own application. To act as an Issuer service, you need:

- A web server where you can serve your JSON-LD files for your Issuer Profile, BadgeClasses, and Assertions at stable URLs
- Recipient email addresses (other Recipient identification options are coming in the next version of the Specification around the end of 2016)

Additionally, for signed Assertions, you need to: * Generate a public/private key pair and host the public key * Sign the badge Assertions when they are issued

https://github.com/mozilla/openbadges-backpack/wiki/Issuer-Checklist

Validation

To determine the **credibility of an Open Badge**, Consumers can **inspect and validate the badge with an Open Badges validator tool**, often one built into the display platform where they see a badge, to determine whether it's valid, and that it belongs to the expected Recipient.

A good Open Badges validator ensures a number of checks pass:

- Validation that the badge is awarded to **the expected email address** of the Recipient:
- Validation of **expiration**: Open Badges may have expiration dates, allowing organizations to issue badges for skills or authorizations which are only valid for a set period of time. Validators will check that a badge hasn't expired.
- Validation of **Structural validity**: Badge metadata should be properly structured according to the Open Badges Specification, including relationships between components to detect integrity problems that may indicate foul play.
- Validation of **Issuer identity**: Open Badges contain profile information about the Issuer who awarded the credential, including contact information if additional questions arise. Good validators make it easy for Consumers to see the relevant information about the Issuer profile and the issuing platform, software, or service used by the Issuer.
- Validation of **cryptographic integrity**: For badges containing cryptographic signatures, these signatures are validated and information is displayed about the provided public key and relationship to the Issuer profile.

https://openbadgesvalidator.imsglobal.org/

When a badge is awarded to an earner, these typical steps may be carried out:

- Issuer creates and hosts a badge assertion
- *3 hosted JSON files OR a JSON Web Signature describing the badge award*
- *Metadata should not change after the badge is awarded*
- *Includes the earner identity info*
- *Assertion includes badge class, either as a URL or an inline object*
    - *Badge class describes what the badge represents and includes issuer organization*
        - *Issuer organization describes who issued the badge (can be a URL or inline object)*
- Issuer offers to push the earner's badge to their Mozilla Backpack
- *here the earner can decide whether to make the badge part of a public collection*
- Displayers query the earner's Mozilla Backpack (or another resource) for badge assertion info
- *Displayers can only query for badges the earner has chosen to make public*
- *Identity can be verified, as can signatures where appropriate.*

Before serving or displaying an assertion, issuers and displayers can use the Validator to check that the structure is correctly formed - the tool works for both signed and hosted assertions.