Professional
Examination Service
Credentialing Insight

Digital "Badges" Emerge as Part of Credentialing's Future

Frank Catalano and Kenneth J. Doucet
Professional Examination Service

August 2013

Professional Examination Service
475 Riverside Drive, Suite 600
New York, NY 10115
212. 367.4200
www.ProExam.org

Consider this scenario:

> *Megan is looking for a job in web design. She's experienced in Ruby on Rails – a website programming language – but she learned it on her own. As she reaches out to potential employers, she wishes there were a better way to prove her depth of knowledge so she'd stand out among other candidates.*
>
> *Ben's company is looking for website programmers. His inbox is crowded with resumes and portfolios. The candidates all tout various programming skills, but Ben can't know for sure that those skills are at the level he needs, or that they're even true. He doesn't have a quick way to verify them.*

Situations like Ben's and Megan's have been common for decades. A job seeker wants to prove that he or she has certain skills, and the employer has to trust that what candidates include on their résumés is true.

This is now changing with the emergence of **digital badges**.

The digital badge is rapidly gaining traction as a new representation of a credential and has the potential to become an accepted marker of knowledge, skills or achievements – up to, and including, any type of professional credential.

What is a digital badge?

The concept of a badge is familiar to anyone who ever was in Scouting: learn or demonstrate a skill, earn a merit badge. But rather than requiring cloth and a needle to apply, these new badges are purely digital, and can be shared with potential employers and on social networking sites.

They are also verifiable. Each of the newest digital badges is embedded with unique information and links to an issuing organization, so everyone viewing the badge can be confident that it represents the skills of the individual who earned it.

Old vs. new: the evolution of digital badges

Most of us have seen older versions of digital badges on websites. Historically, these were static graphic images, and may have been earned for completing training or sitting through an online course. The old-style badges lacked critical characteristics that would give them real value to both the earners and the people they hoped to impress.

Old digital badges: Problems

- No easy way to verify how the badge had been earned.
- No proof that that the individual displaying the badge was the person who earned the badge. (When a badge is just a graphic, it's simple to digitally cut and paste it anywhere.)
- No mechanism to share and display the badges outside of the closed systems that issued them.

In essence, the old badges have the same issues that any standard résumé carries: just because a candidate lists a degree, a certificate or a grade point average, that doesn't mean it's accurate. In addition, degrees and certificates listed on a résumé aren't immediately verifiable, nor do they necessarily provide a comprehensive picture of what that person has achieved.

New digital badges: Solutions

So how does the new breed of digital badges solve these issues? They contain critical features that static, image-only badges lack.

- Metadata embedded inside the image ties the badge back to how it was earned by the individual, and to the issuer.
- Technical standards make it easy for those who have earned badges to share them.

A quick history of digital badge development

These new digital badges aren’t yet commonplace. The first push to create badges began as a way to recognize achievements or informal learning that happened outside of educational institutions, or to capture smaller chunks of education or skills that didn’t neatly fit into the current model of transcripts or degrees. These early badges were digital, but generally were just static images.

The non-profit Mozilla Foundation subsequently spearheaded the current push. Within the last several years, Mozilla, an organization best known for the Firefox web browser and which has a stated mission of promoting “openness, innovation and participation on the Internet,” has been the most visible organization developing and advocating for the use of new digital badges.

The MacArthur Foundation stepped in as a major funder and partner of Mozilla’s for further development of digital open badges. In 2011, MacArthur held a competition and awarded funding to a wide variety of organizations, including winners with familiar names such as NASA, Disney-Pixar, and – not surprisingly – the Girl Scouts. Other winners were organizations that developed direct workplace applications: BadgeWorks for Vets, which gives returning military personnel badges to represent military skills and training for use in applying for civilian jobs, and the National Manufacturing Badge System, which under the aegis of the National Association of Manufacturers and its non-profit Manufacturing Institute recognizes advanced manufacturing skills obtained by both students and workers.

Since then, the technology and standards behind new-style digital badges has been further driven forward (with continued support by the MacArthur Foundation) by Mozilla. Mozilla calls its digital badges “open badges” because the technology to create them is open technology, representing “an open source model (that) means that improvements made by one partner can benefit everyone, from bug fixes to new features.” In the process of working toward the first official, version 1.0 release of the Open Badge Infrastructure in March, 2013, it became clear that an open digital badge offered a mechanism for representing skills, knowledge and accomplishments that extends far beyond hobbyists or self-motivated learners.

And, under the Open Badge Infrastructure, these digital badges – even those earned from different issuing organizations – can be combined, or stacked, and easily shared on job sites, social networks and directly with employers. Those with open badges can store them in a “digital backpack” or “digital vault” – a virtual lockbox where individuals can keep all their badges in one place and share them as needed.

How digital badges will work

In the example of Megan, the web programmer, here’s how she could earn and use a digital badge.

1. Megan searches for a respected badge issuer.

   Megan knows Ruby on Rails, but she thinks she’d be a stronger job candidate if she could demonstrate her knowledge and skill with an online credential. She finds a respected online education provider that issues digital credentials for Ruby on Rails.

2. She decides whether or not she needs to take a course before an online test.

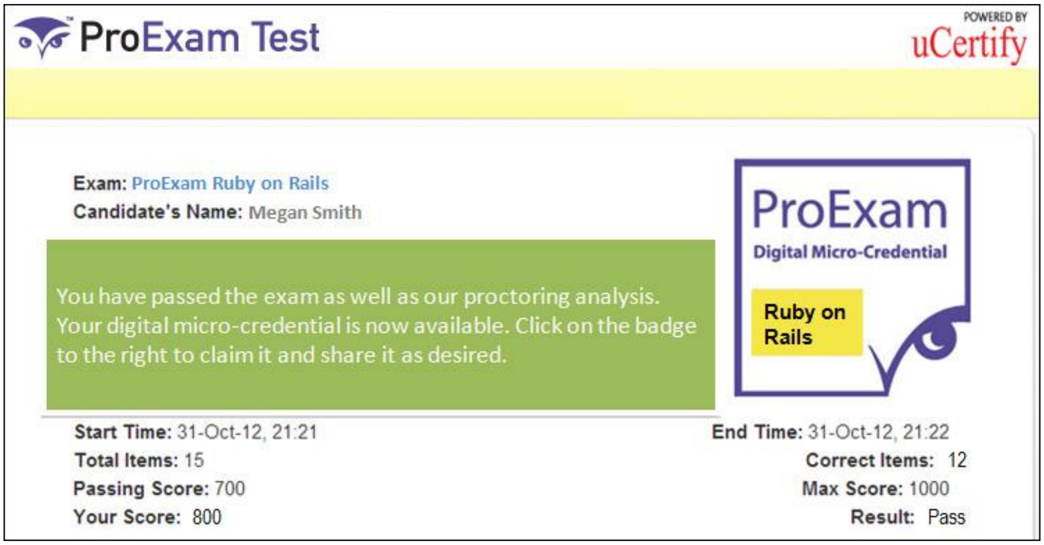
   Megan is able to take a practice test on the issuer’s site which helps her decide whether she needs to take an online course, or whether her knowledge and skills are already sufficient to pay for and take an online test.

3. When Megan is ready, she takes a digitally proctored, online test.

   Megan’s online test is remotely proctored, a way to ensure that Megan is the person taking the test, not anyone else, and the final results will be issued only to her.

4. Megan passes the test and earns a digital badge – a credential that confirms she has the knowledge and skills for a specific level of the Ruby on Rails programming language.

   At the end of the test, Megan receives notification that she’s passed the test. She receives a digital badge – a credential that is tied to her, as the earner, and also to the issuer. She stores this badge in a digital “backpack” where she can add and stack other badges she earns.



Exam: ProExam Ruby on Rails
Candidate's Name: Megan Smith

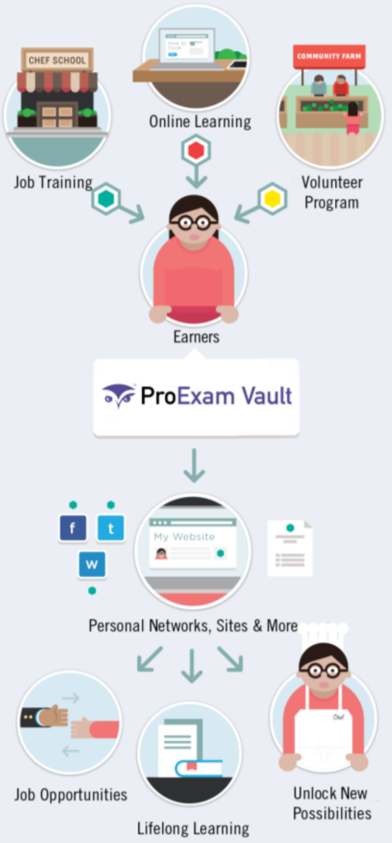
You have passed the exam as well as our proctoring analysis. Your digital micro-credential is now available. Click on the badge to the right to claim it and share it as desired.

Start Time: 31-Oct-12, 21:21
Total Items: 15
Passing Score: 700
Your Score: 800

End Time: 31-Oct-12, 21:22
Correct Items: 12
Max Score: 1000
Result: Pass

5. Megan shares the badge image or link with others.

   Anyone who views this badge, whether it’s on Megan’s online portfolio, on social media pages like LinkedIn or Facebook, or through direct links she sends to potential employers, will get an accurate and verifiable snapshot of her programming skills. If the badge is issued by a credible and respected organization, it will carry more weight with potential employers.



Issuers: Any association, organization or institution wanting to award someone a digital badge.

Earners: Individuals who earn a badge.

Displayers: Web pages where badges are displayed – can be private or public.

Digital Badges: Earned for achievements from an association, organization or institution that issues a badge.

ProExam Vault: Issuers securely manage their awarded badges and Earners store and organize earned badges (in a digital “backpack”).

Employers: Hiring managers verify a displayed badge through its click-through validation page.

Source: Mozilla Foundation, ProExam

So, can Megan do this now? For some skills, yes. Digital badges are a nascent but growing technology. Some organizations are already using them on a small scale, and others are exploring the best way to implement them. All organizations want to know that the badges they issue will be secure.

Authenticating credentials: digital badge security and validation

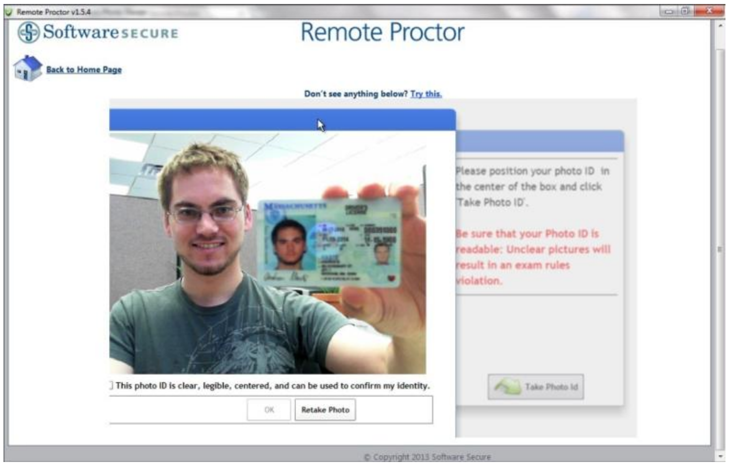
Ben gets an inquiry from Megan about a job in his firm. He sees that she's earned a Ruby on Rails credential, and it's from an organization he knows and respects. But digital badges are new to him. How can he be sure that Megan actually earned the badge? How can he know that it's really from the organization that issued it?

Since digital badges are an emerging technology, potential users often have questions about security. They are concerned that:

- Badges can be "stolen" or misrepresented – a person may not actually have the credentials that he or she displays.
- People will display a counterfeit badge.
- Unscrupulous organizations will issue badges that don't represent the acquisition and demonstration of knowledge or skills.

Specifically, any issuer of a digital badge needs to address three types of security.

1. **Data security.** This step ensures that the digital badging process – from assessment for a credential to the issuance of the displayed badge – cannot easily be hacked, or have any critical aspects modified by an unauthorized party. This is accomplished by the assessment provider and badge issuer adhering to high-level security protocols for exchanging and storing the data that the open badge represents.
2. **Exam security.** If the credentialing process requires an examination, issuers can implement remote proctoring technology. The technology requires that test takers use their computer's camera to prove their identity with a photo ID, and agree to take the exam while the camera records audio and video of the process.



Don't see anything below? Try this.

Please position your photo ID in the center of the box and click 'Take Photo ID'.

Be sure that your Photo ID is readable: Unclear pictures will result in an exam rules violation.

□ This photo ID is clear, legible, centered, and can be used to confirm my identity.

© Copyright 2013 Software Secure

Test taker providing authentication for remote proctoring during an online exam.

Source: Software Secure

3. **Badge validity.** This final type of security means that once an earner claims a badge and publishes or shares it, the image for the badge is far more than a graphic. Embedded metadata in the graphic ties it to both the earner and to the issuing organization. When someone such as a potential employer clicks on the badge image, they'll go to the validation page that is hosted by the issuing organization. There, the viewer will see to whom, for what, and when the badge was issued. He or she can also view when the badge expires, if it requires ongoing activities to maintain (recertification), and if it has been revoked.

Digital badges as credentials

With the technology in place – technology that ensures data and examination security, as well as the validity of the resulting digital badges – organizations can design their own digital credentials. These credentials, represented as badges, can meet a wide variety of needs. For example, issuers can control:

- What kinds of skills, knowledge or experience credentials represent.
- How credentials must be acquired, as well as when, and if, they expire.
- How to systemize, or "stack" credentials.

A credential sponsor can develop a system of credentials in several ways – none of which are mutually exclusive.

For example, an issuer can choose to create a **micro-credential.** Essentially, a micro-credential is a precursor or more granular form of a full, traditional credential, such as those offered by national or international sponsors of credentialing programs. Certain parts of a full credential might be "chunked" to provide a scaffolded starting point for a larger credential. In other cases, an assessment-based micro-credential, created by a credible third party, might satisfy some eligibility requirements for an established credential.

mozilla
OpenBadges

Organizations might also choose to create an **add-on to a traditional credential.** These micro-credentials could reflect additional specialized skills that go beyond the full credential, or reflect accomplishment of a certain number of continuing education units or ongoing professional study.

Finally, issuers can develop **a standalone, new credential**, which they can design to their own specifications, and which reflect an area of practice that is either emerging or not broad enough to merit a traditional credential, yet is in demand by employers or the market.

In all of these cases, the digital badge has the benefit of being purely digital – so no paper handling – and is based on an open standard that no single vendor controls. The information the badge represents can be non-traditional, and represent a wholly new field of knowledge or skill. Regardless of its use, each badge would be fully managed by the issuing organization.

Some examples of potential uses:

- In higher education, a student could earn a micro-credential after completing an assessment for an individual course or set of courses. Eventually, these micro-credentials, stacked together, could equal a type of college degree.
- Computer programmers could earn and collect badges reflecting their demonstrated skills in various programming languages.
- Trade organizations could issue assessment-based credentials showing that members had achieved specific skills.
- Membership organizations could issue specialty micro-credentials. For example, an individual in the nutrition field might someday earn a micro-credential as a "celiac specialist."
- Sales professionals could earn badges for specializations. For instance, a pharmaceutical representative could earn a micro-credential for demonstrating knowledge of a specific disease (such as COPD) or government regulations (such as how to properly handle drug samples).

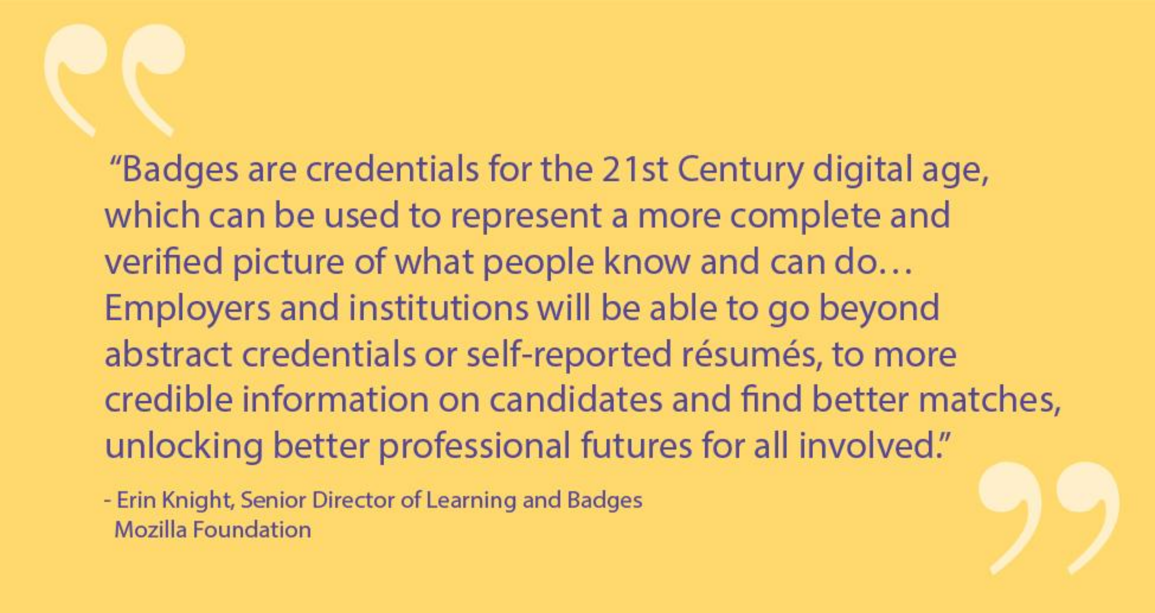
Current uses of digital badges

Although more people are beginning to understand the concept of digital badges, their use isn't yet routine. Many current issuers are using them for motivation, such as rewarding volunteers or participants, while others apply them as simple markers of accomplishments, like completing levels of educational software. To date, digital badges have tended to be given for low-stakes reasons, infrequently backed by an assessment, and not used widely with employers.

However, that viewpoint is starting to change. In a recent research study, in-depth interviews with Fortune 500 senior hiring managers found that companies thought that digital credentials would help them narrow a pool of applicants to those most likely to have the specific skills for a position. The study, conducted by an independent research firm for Professional Examination Service (or ProExam, which was the first professional credentialing services organization to announce plans to design and issue Mozilla-compliant digital badges), also revealed that the promise of one-click, secure verification of a claimed credential – including confirmation of whether the credential was current – eased a pain point for many employers.

In addition to ProExam, the Mozilla Foundation's Open Badges website (OpenBadges.org) identifies several other organizations planning a workforce presence. In addition to the Manufacturing Institute and Badges for Vets, Workforce.io is creating badges for entry-level workplace skills and Coderbits already issues more than 500 badges for software developers and designers.

Finally, in June 2013, former President Bill Clinton endorsed a major program that will get at least two million people started with digital credentialing. The initiative, called 2 Million Better Futures (2MBetterFutures.org), will help students (K-12 through college) as well as workers earn digital badges that will help them further their educational and workforce goals.



> "Badges are credentials for the 21st Century digital age, which can be used to represent a more complete and verified picture of what people know and can do… Employers and institutions will be able to go beyond abstract credentials or self-reported résumés, to more credible information on candidates and find better matches, unlocking better professional futures for all involved."
>
> - Erin Knight, Senior Director of Learning and Badges
> Mozilla Foundation

Issues to consider

As the use of digital badges gathers steam, issuers will need to think through both their implications and applications. In addition, to solidify the use of digital badges as a widely recognized and trusted credential, several pieces need to fall into place.

- Employers will have to value digital credentials as much as they do traditional credentials now. This is likely to happen if digital credentials live up to their promise of security and verifiability. Early research indicates that employers would appreciate the specificity of skills and one-click verification that digital badges represent.
- Candidates will need to seek out digital credentials and micro-credentials that represent skills, knowledge or accomplishments that are important for them professionally, augment traditional credentials, and are issued from a trusted and recognized source.
- Career and social networking websites will need to make it simple for earners to display digital badges. Mozilla hopes to ease this issue with its Displayer API, and by keeping the technology for developing digital badges open for developers.
- Although more semantic than technical, many adopters of the new technology will need to overcome the childhood connotation of the term "badge." That's why some organizations, such as ProExam, have begun calling the workplace versions **digital credentials** or **digital micro-credentials.**

Potential benefits of digital badges

Ultimately, once the barriers are overcome, digital badges could have tangible and unique benefits.

Employers would be able to more quickly identify specific skills they desire in a large candidate pool and more easily verify a claimed credential.

Candidates could incrementally earn a traditional credential, reflect post-credentialing achievements, or create their own by combining several micro-credentials.

Credential sponsors could recognize a multitude of benefits, such as:

- Generating additional revenue by offering assessments and recognition of subject matter concentrations.
- Offering testing in a cost-effective manner with secure, Internet-based testing and remote proctoring.
- Having the ability to monitor and control the status of credentials by building in expiration or recertification dates.
- Building the organization's brand with the ability to offer non-assessment based digital badges as recognition for volunteer efforts as well as assessment-based micro-credentials for highly focused knowledge or skills.

Despite their virtual nature, digital badges may represent the future of credentialing. As our learning landscape shifts from formal and linear to informal and on-demand, and as employers seek faster and more reliable ways to connect with the workers that will add the most value to their organizations, a secure, digital credentialing system is becoming more of a necessity, rather than a novel idea or convenience.

Frank Catalano is the Chief Marketing Officer of Professional Examination Service and is a strategist, author and veteran analyst of digital education and consumer technologies. Kenneth J. Doucet is Director, Enterprise Growth of Professional Examination Service and has spoken on digital credentials and badges at events including the annual conference of the Association of Test Publishers. This paper is based on a shorter essay that appeared in the Institute for Credentialing Excellence's ICE Digest newsletter, Summer 2013 issue.

Professional Examination Service (ProExam) is the most experienced organization in professional credentialing, providing comprehensive services and technologies to programs across a broad range of professions. Since 1941, ProExam has supported professional licensure and certification, training and continuing professional education with its full, flexible range of assessment and advisory services. ProExam is a not-for-profit organization with uniquely tailored services, a dedication to personal attention and insight into emerging credentialing trends. Learn more at www.ProExam.org