Forward:

Awards have long existed in both education and employment. Colleges have conferred diplomas that represent the successful completion of a series of course-level requirements. Government, industry and trade groups have issued certifications and licenses to signify competencies and professional skills. However, credentials representing achievement in this context are not standardized, rarely digital, and difficult to share.

Open badges (also known as badges or digital credentials) are the emerging standard for representing certifications, credentials and other skill or knowledge-based competencies within the IT certification industry. Badges are rapidly being adopted within the Information Technology (IT) field by companies such as Oracle, Citrix, Microsoft, IBM and others. Portability, accessibility, security and verification are key influencing factors for IT organizations as they migrate their paper-based method of certificant recognition to a digital-based way of recognizing achievements.

Through this white paper, members of the ITCC, a council of IT industry leaders focused on promoting IT certifications and committed to growing professional certifications, will cover the industry trends around open badging benefits, best practices, outcomes, security considerations, pitfalls, and platform technology options. The intention of this paper is to cover the industry trend around the transformation to digital credentialing. It is the hope of the ITCC that after reading this paper, one will not only have a stronger understanding of badging, but the measures that must be in place to both successfully promote and protect a badge’s worth.

Section 1: Introduction to Badging

The History of Open Badges:

IT certifications were introduced in the late 1980s with the Novell Certified Engineer program. By the turn of the millennium, dozens of organizations offered IT certifications to over a million professionals. But each IT certification issuer stored the data about its certified professionals in proprietary systems, making it almost impossible to share an official certification transcript. In addition, employers had a difficult time understanding the capabilities of those certified professionals.

In 2011, the Mozilla Foundation and the MacArthur Foundation came together at the center of a broad community of collaborators to produce an open technical standard for any organization to create, issue, manage and verify digital badges. In 2012, they released the first version of their open badge specification and the Open Badges Infrastructure (OBI) software that implements the standard.

Between 2013 and 2015, digital badges gained momentum as several IT credentialing programs, such as Adobe, Citrix, Oracle and IBM adopted the technology and began offering badges to their certified professionals. Badges are poised to continue this positive trajectory into 2016 and beyond as their benefits to issuers, earners and employers become more visible in the marketplace.

While many certification holders find badges to be preferable, due to their ability to quickly manage and display their qualified skill sets to prospective clients and employers, credentialing programs (along with the employers, themselves) have hesitated to hold badges in the same light as the more traditional certification. This hesitation has been due largely to the need for a standardized system of verification. This system will, in turn, provide a strong way for employers and credentialing programs to verify that an individual’s achievements are indeed legitimate. In recent months, the industry has made great strides towards defining and implementing tactics to add verification to a large majority of currently issued badges.
Elements of Open Badge Metadata:
• The defined outcome required to earn the badge and the evidence earners provided to demonstrate their competence
• A direct connection to the credential issuer
• The relationship between the badge and larger programs, professional learning pathways and larger skill sets
• Verification of the badge earner’s identity and relevant, secure, trusted communications about their qualifications, competencies and skills.

Benefits of Badging to Current and Future Certified Professionals:
The value of certification continues to increase as the global job market demands a workforce fluent in the most current skills. With this demand for job-ready individuals, badges provide credential issuers with several key opportunities to:
• Streamline the credential fulfillment process, while recognizing cost savings
• Expand the reach of their brand while ensuring its integrity in the digital space
• Create clear connections between their credential and employability
• Replace a paper certificate with a digital artifact that is always verified

At the same time, badges provide earners with the modern recognition for the achievements they need to participate in a professional landscape that is ever more digital in nature. With a digital badge, earners can:
• Broadcast their skills and achievements to popular professional and social networking sites such as LinkedIn, Facebook and Twitter
• Provide potential employers and others within their network the full context of their professional abilities
• Take ownership of their credential and the verification process

Through the badging system, employers determine which skills and credentials are necessary for a given role. Digital badges, in turn, create a level of transparency that enables the employer to quickly and accurately assess a candidate’s abilities and qualifications for a position. Badges provide employers with the ability to:
• Verify a credential status, quickly and easily
• Use badge metadata to clearly understand an individual’s competencies
• Expedite the hiring process

Section 2: Sampling of Badging Platforms

A badging platform is a cloud-based technology that serves credential issuers, earners, and employers. The platform allows issuers to create badge images and metadata, track and report on analytics, and supports issuing and maintenance of the credentials and earners. The platform also provides an interface for earners to manage data privacy and sharing of their credentials, and allows employers to access the verified data with the earner’s consent.

Several platforms have led the way for credential issuers, earners and employers to tap into the benefits that badging affords.

Acclaim is a product of Pearson, the world’s leading learning company, and is a top issuer of badges that recognize professional achievements from respected brands across a variety of industries. With a robust suite of reporting and analytics tools, Acclaim offers badge issuers and earners the information they need to make an impact on the global job economy.
**BadgeCert** is a recognized leader in digital credentialing and professional recognition for associations, trainers, corporations and universities. BadgeCert’s enterprise-class platform helps move careers forward by facilitating the creating, issuing, managing and sharing of digital badges that verify earners’ skills, credentials and experiences with a single click.

**Mozilla Open Source** is free software and an open technical standard any organization can use to create, issue and verify digital badges. The reference technology and enhancement roadmap are maintained by contributions from a community of Open Badge activists, referred to as the Badge Alliance.  

### Section 3: Benefits of Implementing Badging

Badging is about an individual's journey toward gaining greater skills or promoting the skills that they have already acquired while also enabling the entire IT Certification ecosystem in bettering their processes and strengthening the workforce. Through badging, the individual badge holder, employer and even the certification programs benefit greatly in their own unique ways:

**For the Issuing Certification Programs:**
- Increased brand recognition
- Better access to talent through the organization’s ecosystem
- Cross-promote other products
- Continuous verification protects the value of the brand and the credential by reducing fraud
- Ability to promote and encourage skills progression
- Reduce fulfillment cost

**For the Badge Holder:**
- Promote their learning and achievements using social media
- Identify a new or better career pathway
- Identify further training/learning opportunities to advance their career

**For the Employer:**
- Recruit and hire the right talent faster and at a lower cost
- Verify resume education and skills claims quickly and securely

Through these added benefits, all members of the IT Certification world will benefit greatly once longstanding certifications are successfully transferred and recognized within the more modern badging platform.

### Section 4: How Can Badges and Certifications Co-Exist?

The IT Certification industry is currently divided. While many well-respected members of the industry are more comfortable with the traditional certification approach, just as many are intrigued by the possibility of redefining the industry through an open badging platform. Through countless discussions at small and large-scale industry gatherings, multiple methods of blurring the lines between certification and badging have risen to the surface, some of which are already in practice by major certification programs.

One method employed by some IT certification programs, is to use badges solely as a digital representation of the certification, choosing to badge all of their certifications or just a subset of them. In this instance, an individual can click on the badge in order to verify the candidate has actually
earned the certification. It also provides an easy mechanism for sharing the new accomplishment via social media or email. Some organizations may opt to pilot certain certifications for badging rather than opening up all certifications right away.

A second method, is to use badging to represent a nano (specialty) credential as part of a learning or skills progression roadmap. In this instance, a certification program may choose to badge knowledge attainment (such as the completion of a course) or skills recognition (such as the creation of an application). Research shows that individuals prefer to absorb information in small increments. Therefore, by encouraging the candidate to slowly achieve his or her certification through nano credentials, the certification program may ultimately see a rise in issued certifications because the candidates have received recognition throughout the progression of their roadmap and are more likely to complete the full course.

As badges become more prevalent in social media, their relative value and positioning in the IT industry will be increasingly difficult for candidates to understand. The larger problem remains for employers—how do they differentiate from badges acquired only by attending a class or those earned by proving skills in a high-stakes assessment? It will be up to vendors and badging platform owners to cut through the confusion if badging is to be effective and embraced by the IT industry. These stakeholders must construct simple and compelling guidelines describing how each badge fits into the larger picture of a candidate’s journey. Whether badges represent large achievements like certifications or motivational awards for completing smaller tasks, they should complement each other. Setting up badges as competition to traditional certifications could divide candidates and undercut the adoption rates of both going forward.

Section 5: Potential Risks

Many IT credentialing organizations currently offer badges for recognized, high-stakes certifications. With such familiarity in the IT community, there are few risks for an IT company to introduce badges for its certifications. In contrast, there are fewer IT credentialing organizations offering badges for activities other than certification and variation amongst those companies on what is badge-worthy. As a result, non-certification badging carries additional risks.

Risks of Badging in Certification:
In a certification-only scenario, the two key risks revolve around monetization of badging and continued relevance of certifications.

There are two motivating factors to monetize certification badges. First, building or acquiring a solution which issues badges that the industry would find trustworthy and useful can involve significant costs. Engineering effort is required to produce a system that provides an acceptable level of authentication for user credentials and delivers useful business intelligence data to the badge issuer.

Secondly, the ability to share verified badges could be seen as a premium service, much like printed certificates and wallet cards. However, issuing companies should consider that enabling credentialed individuals to more easily share their accomplishments online could result in a boost in marketing that outweighs the investment.

On the issue of relevance, there are also two points to consider. First, without a digital representation including verifiable metadata, even cutting-edge technology certifications may lose visibility and associated value by both individuals and the companies that hire them. Both audiences need
streamlined, online ways to share and search for proof of technical competence.

Also, once an issuing company decides to offer digital badges, the challenge becomes one of selecting the right set of certifications to badge. The most common approach used by early adopters of digital badges in the IT industry is to offer badges for certifications currently in market (vs. legacy certifications). However, there is also the opportunity to further limit the badges to drive adoption and competence in key strategic technology areas (e.g. Big Data).

Risks of Badging in Non-Certification Scenarios:
With digital badges comes the opportunity to showcase additional credentials earned by individuals during their path towards technical mastery. These credentials could be awarded by completing learning-related activities other than proctored technical exams, and will involve lower-stakes assessments or other validation. In these non-certification scenarios, there are a number of potential risks that credentialing bodies should take into account:

Awarding the Right Activities: Surveying the market on how credentialing organizations use badging reveals two primary categories of badges: those related to acquiring and validating technical skills (i.e., skills badges) and those related to participating in community activities (i.e., participatory badges). Within these categories, one can find multiple levels of activity that each result in a badge, from a lightweight activity, (such as website registration) to a significant activity, (such as presenting at a users’ conference).

One use of badging is to drive continuous engagement with customers, for example, through a technical support website. If this is the sole intention of the badging organization, then the full range of activities can be considered for badging, coupled with a user loyalty and gamification solution.

However, if the primary intent is to complement technical certification, then the badging organization should consider limiting the issuance of badges to “résumé-worthy” activities, which would reflect well on them and their customers when shared on professional sites, such as LinkedIn.

When striking a balance between these two uses, there is a risk in defining badges of the right size that encourages users to seek attainment while still adding value to their professional development.

Over-Proliferation of Badges: Once organizations decide on the categories of badges that are most useful to their customers, they must determine the number of badges to be offered in each category. If too many distinct badges are offered, showcasing the value of a given badge becomes difficult, resulting in dilution of the brand. To that end, the organization should first consider locking on the definition of a core set of badges that would appeal to the majority of their customers. This should be followed by a metered release of specialty badges, with prudent removal from market if the forecasted popularity goal is not met.

Balance Between Badges and Certifications: For organizations that decide to implement skills badges, the decision must be made on how these credentials relate to formal, technical certifications. Early adopters of badges in the technical credentialing community have taken a number of different approaches. Some offer badges that are completely separate from technical certifications, while others use technical badges as a prerequisite to certification, in place of lower-level exams. Still, a third segment use technical badges for post-certification specialization or continuing education, in place of recertification exams.

Clear messaging on the relationship between skills badges and certification is critical, as customers
and hiring managers will want to understand the equivalency between traditional certifications and these new skills badges, and raise concerns about the value of certification if lower-barrier credentials are simultaneously offered.

**User Authentication and Piracy:** As badges could be awarded by completing learning-related activities other than proctored technical exams, they will involve lower-stakes assessments or other validation. Badging organizations, therefore, run the risk of issuing credentials to individuals whose identities have not been robustly verified. To address this issue, badging organizations should consider implementing an audit program and/or requiring at least proctored activity before awarding the associated badge.

An additional risk is that badges could be reproduced and circulated to unauthorized individuals. This can be addressed by building or acquiring a badging solution that associates verifiable candidate-specific metadata to the issued badge.

**Monetizing Non-Certification Badges:** When issuing badges, the question on if and how to monetize needs to be answered. If the technical badges ultimately lead to certification, then there is a motivation to issue these badges themselves without additional costs. However, without a price tag, the perceived value of the badges may be lower.

If the decision is made to monetize badges, then the organization must determine at what point along the path towards earning the badge that monetization should take place. If the badge is purchased once all of the contributing activities are completed, the price of the credential may seem cost-prohibitive to customers before they even start on their path. There are lessons to be learned from mobile app purchasing behavior, where customer spending on micro-transaction in-app purchases is often greater than initially buying the full version of the app.

**Timeline for Introducing Badges:** Once an organization decides to offer skills badges that are associated with certification, there is a challenge of establishing the schedule for introducing them to their customer community. A balance must be struck between attracting new entrants while maintaining the established base of credentialed individuals. If the switch to a badge-centric validation model takes place too soon, the organization runs the risk of disenfranchising the pool of customers who completed the standard certification path. If the switch occurs too late, the organization may lose the interest of new entrants that are looking for their first technical credential without the investment of a full certification.

**Section 6: Security in Digital Badges**

**The Importance of Secured Badges:** Test security and credential validation have always been important inputs into a credible IT certification program. For a certification to add value to individuals and employers, it must come from a trusted entity and make clear what the earner can do as a result of earning the credential. Easy verification of the credential also plays a crucial role in the overall security of IT credentials.

Without a clear level of security and verification, a credential will be devalued and not trusted in the marketplace. That is why ensuring safeguards are in place around a credential issuer’s badge program is incredibly important.

Credential security is of special interest to the ITCC, made evident through the Securing Certifications Initiative. With this in mind, the ITCC is providing thought leadership around the enhancements and
possible detractors of security within digital badges.

**Badges Provide a New Level of Transparency and Security to IT Programs:**
Badges are not just a trendy way to expand the reach of a credential issuer’s brand, or to engage with credential earners in new ways. They provide vital secure checkpoints online that will strengthen the integrity of credential issuers in the digital space. There are three key aspects to badge security that are not available through traditional paper-based forms of recognition:

- Unique metadata that connects each badge to an individual
- Real-time verification
- Issued from a trusted source, not self-populated on a résumé or LinkedIn

**Unique Metadata:**
Metadata, defined as information that is held as a description of stored data ensures that no one can impersonate a certified IT credential holder online. Although badges are simply digital image files, they are linked to verified data that makes them more reliable and secure than a traditional paper credential. When issued from a trusted IT organization, digital badges protect not only the organization’s stake in IT certification but also that of the individual earner.

**Real-Time Verification:**
Badges can be easily verified simply by clicking on the badge image, which is a time saver for all active parties in the IT certification ecosystem. By clicking on the badge, a viewer is taken back to the badge’s source of truth: the platform or information repository where metadata is stored. Single click verification provides instant access to the full details of a credential such as:

- Issuing organization’s name
- Credential holder’s name
- Issue and expiration dates
- Clear description of what was done to earn the credential
- Evidence associated with earning the credential
- Associated skills and certifications

**Issued from a Trusted Source:**
By nature, digital badges can be issued by anyone to anyone. That’s why it’s incredibly important to the security of an IT credential for the issuing organization to take control of the badging process. Many résumé platforms allow individuals to self-populate the details of their education, work experience and certifications without requiring proof or verification of the accuracy of those claims. This practice can erode the security—and overall value—of a credential. By offering digital badges directly to credential earners, IT programs ensure that their badges are recognized as coming from a trusted source: themselves.

**Security Considerations Around Badges:**
The ITCC understands that the newness of open badges requires diligent oversight and constant review of the technology and its application to ensure top security. At this time, two main concepts have emerged as security considerations to watch:

- Not all badges are created equally
- Badge falsification
Not All Badges are Created Equally:
We touched on the idea that digital badges can be created by anyone and issued to anyone. There are many badging platforms, many of which do not align with or support the secure, trusted nature of an IT certification. Some platforms do not allow real-time verification. Others do not provide metadata that fully explains and demonstrates an individual’s abilities.

These less rigorous badges are online, mingling with those that take the validation and security process very seriously; this can create confusion among individuals and employers as to what they should or should not rely on. To reiterate a previous point: that’s why it is essential for an IT credential issuer to take control of the badging process.

Badge Falsification:
Just as individuals can create their own paper certificate and fraudulently pass it off, so too could someone mimic a badge and share it online. Although the safeguards of issuing badges through a respected badging platform that supports the level of security and transparency of a credentialing program will mitigate this practice, it will still happen. Again, that’s why it’s so important for organizations to issue their own badges and control the online presence of their certifications.

With the adoption of badges by IT certification programs, and others across a variety of industries, it is clear that badges are no longer an emerging trend. Badges offer increased levels of online credential security—as well as opportunities for falsification—that create a sense of urgency for credential issuers to take control of badging their certifications. The ITCC will continue to be part of the badging conversation, both from a risk and best practices standpoint.

Section 7: Summary
Digital badging will most certainly continue its upward trajectory throughout 2016 and into the future. However, to continue the advancement of this technology, it is the responsibility of every certification program to ensure their badges retain their value through developing strong programs that clearly relay the value of each badge to certified professionals and their employers. In doing so, both the badging initiative and the IT certification industry will continue to prosper.

Section 8: References