The Death of Paid Standards (and the Birth of New Identity Services)

By Anthony Michael Rutkowski[1]

Over the past twenty years, a combination of industry, technological, and legal developments have effectively ended the viability of standards bodies to charge for their published specifications and related registration information. These trends have been especially significant in the information-telecommunications (ICT) and security fields. This article discusses those developments, why they are essential for industry, government, and consumers, and describes emerging features of next generation standards publishing and related identity management services.

Ubiquity as the measure of success

The development and implementation of standards are almost by definition an exercise in achieving ubiquity. Experts in a particular field meet, share their intellectual property, and agree on common specifications related to the products and services provided. In many cases, the provisions have the force of law – either because the standards were developed by a government agency or are referenced by government in conjunction with various requirements. The intended objective is the achievement of a substantial degree of ubiquity, and the success of standards is effectively measured by that result.

Until comparatively recently, the imperatives of standards development were satisfied through various entities turning standards into a printed product and made available at cost. The most substantial expenses are almost always incurred in the processes of bringing experts together and their contributed time – expenses that are invariably borne by the participants.

Several decades ago, many standards bodies – often connected with other larger organizations – decided that the compulsory nature of many standards combined with the minimal costs in their preparation, could produce significant revenue streams if the standards were sold at substantial prices. As the revenues grew, the associated organizations became ever more dependent on the publication monies and effectively shifted their business models from standards body to for-profit publishers.

These practices were further bolstered by the assertion of frequently dubious copyright claims in the standard – especially important as photocopiers became available to produce additional copies at minimal cost. The resulting paradigm, however, became increasingly at odds with the basic objective of standards making – to achieve ubiquitous use of the standard.

[1] Vice-President for Regulatory and Standards, VeriSign, Inc trutkowski@verisign.com, and co-editor of the draft new standard ITU-T Rec. X.1250, *Capabilities for enhanced global identity management trust and interoperability*.

During 1980s, the standards-making to publisher shift became unraveled by two major symbiotic developments. One was the decision by the ARPA Internet community to place its standards on-line for everyone to find and use. The second was the emergence of a dispersed systems developer culture that collectively moved at rapid speeds and voted on their choice of standard based on immediate availability. The combination of these two developments not only revolutionized standards making, but resulted in profound losses by entire developer communities such as the Open Systems Interconnection world who adhered to the old standards publishing paradigm.

Standards revenues had become wired into many standards supporting organizations as imperatives, and as competition among standards bodies increased, those who chose to charge for their standards were caught in an ascending spiral where the prices were raised ever higher as the demand diminished. Finally, most of these bodies realized that publishing and standards making business models were fundamentally incompatible. Over the past twenty years, many standards bodies adapted. Perhaps the most successful example during the 1990s was the European Telecommunications Standards Institute (ETSI) which also served as the secretariat for the GSM/3G community. It made the bold decision not only to place its standards on-line for free, but to provide added features for developers such as navigation "dashboards," effective versioning of specifications, and a registry for real-time access to standards code modules that facilitated discovery, re-use, and testing.

Ubiquity is also important to enhance the quality of standards. In most standards bodies, the specifications are prepared among relatively small groups, and unnoticed errors inevitably get embedded in the resulting specifications. Rapid, widespread availability among engineering and development communities, including students, often results both in fixing unintended errors as well as enhancing or adding features not previously considered.

Essentially all of the smaller standards forums that came into existence over the past ten years have followed the IETF/ETSI model. Ultimately, the International Telecommunication Union Telecommunication Standards sector (ITU-T) – with its global reach and subject matter breadth – made its standards freely available in 2007 and distributed more of its standards in a single week than during its entire 80 year standards making history.

The only apparent standards body in the field that devolved from un-paid to paid standards is the U.S. telecom industry standards body created in the 1980 with the breakup of AT&T originally called the T1 Committee of the Exchange Carriers Standards Association and subsequently renamed ATIS. Its activities were open and standards were freely available until recently, when their availability was restricted and became subject to significant charges.

Clearly, all standards bodies that have made their standards easily and freely available have significantly improved their visibility and stature in the information telecommunications and security sectors through ubiquitous reference and use. The few that have not, have substantially declined in relevance by almost any measure. As best, these remaining standards bodies persist in their practices only in niche sectors where ubiquity does not matter.

Legal systems altered copyright protection for compulsory standards

Some standards bodies that adhered to the publishing model for their standards sought refuge in a dual pronged strategy of copyrighting their standards to prevent copying while urging government agencies to refer to their standards and make them compulsory.

However, most legal systems embrace the fundamental tenet of public notice of statutory and regulatory provisions. Those who are obligated to follow provisions of the law, must be able to readily discover and obtain those provisions. For this reason, in many countries, laws and regulations are not subject to copyright in order to facilitate their widespread availability.

Over the past several decades, many government bodies began to refer to industry standards and incorporate them as part of their regulatory provisions. This practice occurred as an alternative to the complex and lengthy processes of government bodies themselves developing the standards. When such incorporation by reference occurs – as is frequently the case for telecommunications, networking and security standards – the effective availability of the referenced standard becomes a significant consideration.

Standards bodies typically assert a copyright protection for their published standards to protect the integrity of the intellectual property in the standard. For those bodies that still attempt to control dissemination to garner significant monies, copyright assertion has also been a means to retard subsequent re-copying of the standard – notwithstanding the frequently dubious basis for the copyright given the diverse collective inputs into most standards.

In 1997, a website programmer by the name of Peter Veeck posted a copy on his website of an industry standard that local government authorities had adopted by reference. The standards body sued Veeck for copyright violation, and over the next several years, the case worked itself through the U.S. federal appellate legal process. In a landmark 2001 decision, the entire Court of Appeals for the Fifth Circuit held for Veeck – underscoring the "public's right to know the law," and that he did nothing more than publish what had become the law through reference, and therefore the standard was bereft of copyright protection. On appeal to the U.S. Supreme Court, the Court let the *Veeck Decision* remain effective – at least within the States covered by the Fifth Circuit. The decision also remains the most explicit statement of the judicial system on assertions of copyright protection by standards bodies attempting to constrain secondary distribution of their standards when those standards are incorporated by reference into law.

While it is possible read *Veeck* narrowly, the ever increasing practice of governmental bodies to adopt industry standards as law – coupled with the increasing growth of e-Government practices that facilitate public knowledge of the law and standards through ready on-line availability worldwide – seems likely to result in judicial and legislative bodies favoring a *Veeck* outcome. Standards bodies have effectively been placed on notice that they cannot have it both ways – that is, increasing the value of their work by encouraging adoption by governmental bodies, and then holding the public hostage for significant amounts of money for even a glimpse at the specifications to which the public is expected to adhere.

In many cases, the equation is further tilted in favor of a *Veeck* approach by virtue of the significant participation of government officials in the standards making process. This involvement is especially prevalent where security standards are involved. It seems appropriate if not likely that government agencies will begin embracing the spirit of the law and avoid reference to standards or participating in standards bodies when the standards are not freely available. Society's interest in the development and adherence to those standards far outweighs the comparatively trite interest in some standards bodies trying to enhance their revenue - at the expense of national security and infrastructure protection.

The Next Generation Standards Business, Cybersecurity, and Identity Management

To be relevant today as a standards-making body – especially in the ICT sector – the standards must be made available a few clicks away from the engineers and developers using those standards. Because standards usually evolve over time, that availability must also include any sequence of different versions of the standard and any code modules (typically either ASN.1 or XML expressions) in compilable formats in an object namespace.

However, for many standards, there is an additional product beyond just the standard itself that is rapidly growing more important in today's next generation standards environment – namely the "real-time" availability of implementation variables and identity information created as part of the identifier assignment processes associated with the use of many standards. These additional products deserve substantial attention – especially in a next generation identity management world where the discovery of and access to trusted identifier information is essential for verification purposes.

Standards can be divided into two types: a) those that are static, and b) those that provide for implementation variables and assigned identifiers together with associated registration and publication processes. In some cases, those identifiers consist of very large namespaces and may be highly distributed as occurs with radio call signs, telephone numbers, domain names, email addresses, MAC addresses, and object identifiers associated with public key credentials and product codes.

The namespaces for many standards are so large, that in many cases it is government agencies, service providers, network operators, manufacturers, and diverse Trusted Third Parties who attend to their implementation, rather than standards bodies themselves. In many if not most cases, the rapid verification of those identifiers in a world of autonomous open networks has become a critical element in enhancing the trust and security of information telecommunications networks, infrastructure protection, and national security.

In the days of legacy standards making and service provisioning, the registration and subsequent rapid discovery and verification of identifiers were not important. The standards body secretariats - together with delegated authorities along a hierarchical chain - collectively maintained manual systems and paper based publications of assignment lists. These practices began to change in the early days of the ARPAnet when DARPA provided for contractors whose primary purpose was to

effect registration and on-line availability of identifiers through a Network Information Center (NIC) and Assigned Numbers Authority that operated in conjunction with standards-making processes. In the telecom world, the emergence of an internet-like signalling infrastructure also allowed for real-time exchange of telephone number based identities – which was enhanced with the introduction of number portability.

However, it was the introduction of the ARPA internet's domain name system in the 80s and 90s, followed by the Online Certificate Status Protocol (for verifying PKI digital certificates) over the past decade that have altered the landscape for assigned identifier lookups on a grand global scale and at rates measured in millions per second. Still, there are enormous numbers of assigned identifiers created by standards and maintained by standards-making secretariats that remain difficult to discover and are inaccessible through contemporary structured query-response information exchange protocols. This situation constitutes significant cybersecurity vulnerability and a fundamental impediment to enhancing trust in network infrastructures, devices and services.

In December 2007, the Director of the ITU-T's Telecommunication Standardization Bureau announced an initial implementation of an XML-based "real-time" lookup capability for signalling system address assignments - one of its many registration databases. Recently, the IETF's Internet Assigned Number Authority operated by ICANN has begun implementation of a similar capability on an even more extensive scale. The draft new standard ITU-T Rec. X.1250, *Capabilities for enhanced global identity management trust and interoperability,* strongly encourages these developments as essential for cybersecurity and infrastructure protection.

All of the above needs and trends – combined with the kinds of resources to develop and maintain the necessary robust, secure facilities – suggest the likely emergence of new global-scale identity management infrastructure operated by secretariats as well as specialized Trusted Third Party providers for a fee. The latter will enable standards body secretariats to outsource their registration and verification real-time query responsibilities to such TTPs if they lack the ability or interest to operate their own facilities. Those seeking to register standards-based identifiers and variables will no longer get them for free, but will pay for the real costs in supporting maintenance of the standard together with identifier assignments and subsequent continuing real-time verification queries by users. In many ways, today's domain name and PKI industries have already paved the way by creating the business models and infrastructure for tomorrow's next generation network needs.

These shifts to next generation standards business, cybersecurity, and identity management models will be complex - given the global diversity of the activities. Nonetheless, the shifts are entirely feasible and fundamentally essential.