Dysfunction Junction: Do standards function?

By Benjamin Tomhave – ISSA member, Phoenix, USA Chapter

The value of standards has seemingly fallen off in recent years while the organizations that author them fragment, grow distant, or simply fail to communicate and collaborate. Who will step in and provide the leadership needed to lead us to the next generation?

Abstract

The Internet as we know it is based on myriad standards. Without them we would not have the lives we lead. Yet the value of standards has seemingly fallen off in recent years while the organizations that author them fragment, grow distant, or simply fail to communicate and collaborate. The need for standards still exists, but the path forward seems murky at best. Who will step in and provide the leadership needed to lead us to the next generation?

Joining a standards committee can be a great way to round out a resume. It shows an interest in topics larger than today's problems or just focusing on one's career. It demonstrates an interest in helping the community at large. Or, so we would have you believe until you join a committee and begin to wonder what exactly you have gotten yourself into. After all, nobody tells you before signing up that you also need a graduate degree in *Robert's Rules of Order* or that you will have to become savvy in the ways of politics and bureaucracy. Nor do the brochures for Club Standards talk about how easily one might put one's foot into one's own mouth, alienating friends, making enemies, and potentially limiting one's career.

Surely this description appears to be over-the-top and filled with drama, and to a degree that is a correct assumption. However, to underestimate what all goes on in standards committees – as well as between them – is the making of great folklore and stories for the ages. Where else outside of government can an idea be developed slowly over the course of years and watered down to the point that the resultant standard is already implicitly present in the technology the vendors conveniently pushed in parallel? Yes, that is a cynical perspective, but it is also sometimes accurate.

The real question one might ask is if standards are still a useful concept. Never mind that the Internet exists at the mercy of standards, thanks in large part to the combined, though disjointed, efforts of the IETF, IEEE, ANSI, ISO/IEC, NIST, ARPA/DARPA, and various other international, federal, and private sector interests. Of course, most of these standards are focused outside of security, and thus perhaps represent a more readily useful utility versus security standards. After all, it has been at least a couple years since the last major weakness was identified in TCP or DNS or X.509, right?[1]

The answer to the question of usefulness is that standards are obviously of use. To think otherwise would be beyond cynical and would fail to take into consideration all the good that has come from these disparate efforts. Where the argument on utility breaks down, however, is when there is not a good consensus about the "right" path forward. Security standards, in particular, seem to suffer from this problem, leading us to a situation where vendors compete to dominate a given technical committee in order to see their protocol or solution of choice adopted as a standard (look into the ODF vs. OOXML history as an example of this dysfunction[2]). One must then wonder how it is that we got to this point. Is it really as simple as a lack of consensus?

The truth is likely far less interesting or conspiratorial, but may surprise people nonetheless. The torrid reality is that the world in the modern digital age simply moves too fast for the standards process. Combine this fact with current economic realities and we see that standards are in fact very important, not only to customers trying to buy interoperable products, but also to vendors who are trying to position their products ahead of the competition. At the same time, standards provide a double-edged sword because they potentially eliminate

---

1 Except for talks at Black Hat USA 2009 and DEFCON 17 about defeating SSL/X.509. No big deal, right?

2 Groklaw has extensive coverage of ODF vs. OOXML on its website at http://www.groklaw.net/staticpages/index.php?page=20051216153153504.

> ### The torrid reality is that the world in the modern digital age simply moves too fast for the standards process.

the case for vendor lock-in. Despite vendors being heavily invested in the standards process, there is also a certain danger to their adopting standards through reference implementations and eventual product releases. Standards have historically provided a mechanism for leveling the field of competition, which some would say is beneficial in a capitalist society.

It is then from these stresses that we see the current situation. Vendors want standards because they benefit their products, but they do not want the standards because they also reduce lock-in and increase competition. Customers want standards because they result in improved competition, but oftentimes at the cost of quality and value. More importantly, vendors can easily become absorbed in trying to conform to myriad disparate standards instead of focusing on customer requests and requirements. The resultant mess is a world out of sync with itself all in the name of a process so bureaucratic that it is literally timed with a calendar.

An example: key management standards

One of the best examples of just how insane the standards community has become is looking at standards and specification development initiatives for key management. These standards have been triggered as a direct result of the increased demand for cryptographic services, such as required by PCI DSS.[3] With the increased demand for encrypting data comes the increased importance of proper management of cryptographic keys. These needs oftentimes extend beyond simple public key infrastructure (PKI) to managing large numbers of symmetric keys, as well as providing mechanisms for performing encryption operations either transactionally, transparently, or in batch operations.

For an example of just how complex the key management standards landscape is today, take a look at the list of "Key Management Standards and Specification Development Initiatives" that is being maintained by Cover Pages[4]:

- ANSI X9 Financial Industry Standards
- DMTF Security Modeling Working Group
- GlobalPlatform Key Management System
- IEEE P1619.3 Security in Storage Working Group (SISWG), Key Management
- IETF Provisioning of Symmetric Keys (KEYPROV) Working Group
- ISO/IEC 11770: Key Management
- KeyGen2: Key Provisioning/Management Standards Proposal

- National Institute of Standards and Technology (NIST)
- OASIS Enterprise Key Management Infrastructure (EKMI) Technical Committee
- OASIS Key Management Interoperability Protocol (KMIP) Technical Committee
- Sun Crypto Key Management System (KMS)
- Trusted Computing Group: Infrastructure Work Group and Key Management Services Subgroup
- W3C XML Key Management (XKMS)

For those keeping track at home, that is a list of thirteen (13!) different standards and specifications addressing key management – and that list is not even complete! Notice that OASIS itself has two committees on the topic,[5] working at times to separate, yet related, yet occasionally overlapping, ends.

In light of the above list, where is the benefit to customers, vendors, government, and the public at large? More importantly, to whom do you listen and on what topic? Assuming all of the above standards reach final, released states, then which standard would you, as a customer, expect vendors to implement? How do customers even know which standards are important?

Unfortunately, as customers, we often rely on vendors to tell us what is and is not important from an interoperability standpoint. After all, one of the primary benefits to customers is using standards to ensure that two products from competing vendors can be used together (e.g., IPSEC and VPNs). Given the above slate of competing and/or complementary standards, it seems unlikely that either customers or vendors will stand a fighting chance in the short-term. Overall, it seems likely that certain standards will rise to prevalence, not the least of which thanks to multiple vendors adopting them.

Muddling through

As a potential customer, how do you decide what standards are important, what standards are not (as) important, and what to press vendors to support? The answer to this question is not trivial. The worst possible answer is to require customers to become expert in each standard, which simply is not reasonable. Alternatively, customers can try to help each other out, though this could also lead to conflicts of interest for companies that are themselves in competition.

Taking the example of the key management standards, let's go through a quick analysis to see if some clarity can be found. As a reminder, look above to the enumerated list of standards.

The first targets we can eliminate are vendor-specific standards and standards from organizations outside our sector. For the purposes of this example, let's assume a generic non-financial services sector that prefers vendor neutrality and that is interested in symmetric key management. As such, we can eliminate Sun (vendor-specific), GlobalPartner (specific to smart cards), DMTF (their angle is unclear), ANSI X9 (useful information, but it is specific to financial services),

---

3 See https://www.pcisecuritystandards.org/ for more information.

4 Cover Pages Topic Document, "Cryptographic Key Management," Cover Pages – http://xml.coverpages.org/keyManagement.html.

5 Full disclosure: the author sits on both the EKMI and KMIP technical committees.

KeyGen2 (seems specific to PKI), NIST (specific to federal sector – excellent resource, especially for writing security policies, but not pertinent here), W3C (working group charter expired in December 2005), Trusted Computing Group (standard appears to pertain to drive solutions), ISO (specific to 11770, there seems to be a lack of consensus), and IETF (KEYPROV just deals with key distribution). The original list can then be shortened to the following based on these criteria and observations:

- IEEE P1619.3 Security in Storage Working Group (SISWG), Key Management
- OASIS Enterprise Key Management Infrastructure (EKMI) Technical Committee
- OASIS Key Management Interoperability Protocol (KMIP) Technical Committee

In a matter of about fifteen (15) minutes of Internet searches and intuitive analysis the original list of potential standards has been cut by approximately 77%. Now the fun part begins. Or so you would like to think, except for one problem. If you look closely at the three remaining standards you will find that none of them is released yet. Fast-forward through the research process and you will find the following:

- EKMI has had a draft since January 2009, but it lacks adequate reference implementations. It lost key leadership coincidentally with the launch of the KMIP technical committee.
- KMIP has a draft, has strong vendor support, and is moving forward assertively.
- P1619.3 has encountered a few setbacks and is clearly not on track with the schedule asserted in June 2008.[6]

After all this research, most customers would be disheartened. From an initial list of thirteen potential standards, only three hold true potential for ensuring interoperability and cooperation among vendors, of which only one is on-track to be released in the near future.

Is there hope?

The good news, however, is that there is a clear leader in the key management standards race. Unfortunately, it may not be the standard you would choose based on technical merits. In fact, as is often the case, the trip to standardization is often one fraught with consensus and the watering-down of what were originally good ideas.

To top things off, despite filtering the list to a clear leader, we have also uncovered a couple interesting problems: relevance and performance. In the first case, many of the standards did not have immediate or apparent relevance to the project at hand. In fact, one could go so far as to say that very few standards were truly applicable to "symmetric key management" – particularly not from an enforcement standpoint. Certain standards, such as from NIST and ISO, provide good refer-

ences for many aspects of cryptographic key management, but not to the degree of ensuring conformance. NIST Special Publication 800-57 provides a very thorough set of guidance for key management throughout the entire key life cycle, but you will be hard-pressed to find a certification process supporting it in the commercial sector.

Performance is the other problem that seems to plague standards committees. In this context, performance relates to the work being doing and the time frames assigned for completing that work. Standards are not generally run on strict schedules and are limited by the attentiveness of committee members. The OASIS EKMI and IEEE P1619.3 committees provide excellent reference cases for what happens when key leadership changes or when lead vendors modify their role in the process.

In contrast, the OASIS KMIP committee appears to be making excellent progress, but that is for a very specific reason. A handful of key vendors – many of whom were involved in P1619.3 and/or EKMI – got together on their own, drafted a standard, and then came to OASIS and asked to have a new technical committee launched. Thus, vendor support already existed to a high enough degree to nearly guarantee the swiftest process possible. That being said, it will still take the committee somewhere in the range of 18-24 months to take the standard to a final release state.

To top all of this off, consider the working groups that are developing standards, but without much visibility. The IEEE Key Management Summit held in September 2008 revealed this situation quite plainly. Many organizations wanted standards for key management, and yet many of the standards committees wanted their own standards to take precedence, despite the pre-existing work of other committees. Or, in other cases, certain committees had standards complete or in draft that, had they been known and recognized, could have provided a solid basis for cooperation. Unfortunately, some working groups simply had not been engaged by other standards organizations, or vice versa.

All of these observations paint a rather bleak picture of bureaucratic and dysfunctional practices and organizations plagued by in-fighting and painfully long development cycles. More importantly, customers are more-or-less at the mercy of the vendors, entrusting them with making decisions that will hopefully be in their best interest rather than their own self-interest. To top it all off, as in the case of KMIP, one is left to wonder if standards prevail because of the mandate of the most successful vendors rather than because of the virtues of the standard itself.[7]

A path forward?

Given the apparent dysfunction within most standards organizations, combined with the significant degree of overlap

6 Luther Martin, "Key-Management Infrastructure for Protecting Stored Data," *IEEE Computer*, Volume 41, Issue 6 (2008) – http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?tp=&arnumber=4548189&isnumber=4548155.

7 Please note that this is not a criticism or observation of KMIP or the vendors supporting it. Rather, this is a general observation noting that KMIP is successful because of the drive of the large vendors that drafted it and are shepherding it through the OASIS process.

or competition, one is left to wonder if there might not be a better way to do things. Businesses operate under deadlines; why do standards committees not operate similarly? Many business decisions are made based on the apparent merits of the situation, so why do standards not benefit from a similar approach?

It would appear that the various standards organizations and processes could benefit from a degree of consolidation, collaboration, and some form of central leadership. The goal of such a central organization would be to globally coordinate development of standards, de-conflict standards that are on similar paths, bring participants together in a cooperative and collaborative manner, and work toward greatly improving communication, not only between vendors and committees, but also with customers. Too many announcements from too many organizations and vendors can actually serve to muddy the waters rather than provide a clear picture of the best way forward.

Unfortunately, this notion of having some central organization in charge is a naïve pipe dream. Given the competing interests of corporations and governments, it seems unlikely that all interests could be equally represented in an independent organization charged with coordinating all standards activity. As such, this leads to a counter-proposal: a single organization charged not with leadership but communication, cooperation, and collaboration. Specifically, such an organization could exist in order to monitor all standards activity, inform committees and organizations of activity, summarize the activity, and provide free and open analysis specifically targeted to customers.

If a tree falls in the woods…

In the end, one must wonder if there is enough interest in standards from the core constituency (customers) to justify creation of an organization that would be charged with monitoring standards organizations, encouraging collaboration and cooperation, and with providing expert analysis of current standards processes and drafts. More importantly, one must wonder just how this organization would be funded.

In general, it's unclear if the core constituency even cares. Do standards matter to the average enterprise? Interoperability is a frequent target for criticism of vendors, as is vendor lock-in, but to what end? Are deals being lost because of a failure to conform to standards? It seems logical that standards do serve a role once a tipping point is reach, but it's unclear how often these points are reached, or if it is frequent enough to be considered a pattern of good practice.

Yet imagine a world without standards. The Internet as we know it today…the digital age as we know it today…the entire computing age…none of it would exist without standards such as TCP/IP, Ethernet, 802.11, Peripheral Component Interconnect (PCI), Universal Serial Bus (USB), CAT5 and CAT6, RADIUS, Kerberos, LDAP, ATX, SCSI, IDE, PATA, SATA, and so on. Clearly the world has benefited from standards, whether or not the core constituency realizes.

Summary

Overall, standards are beneficial to society. However, the processes are plagued with bureaucracy, the development time lines are very long, and there is a general lack of interest from customers in the development process. There is demand for interoperability and cooperation, but no engagement beyond that point, leaving vendors to battle each other to achieve market superiority and prevalence. In many cases, standards are as much about de facto market position as they are about the development of meritorious and mutually beneficial frameworks.

The standards development process, vendors, and customers would benefit from an over-arching organization charged with monitoring standards processes, encouraging and coordinating collaboration and cooperation, and with providing expert analysis and recommendations. However, funding such an organization would likely be a daunting challenge, not the least of which being because it could serve to work against the self-interest of the vendors who would most benefit from the existence of the organization.

Unfortunately, the disparate and dysfunctional nature of the myriad standards bodies leads to excess market confusion. Too much competition amongst standards can lead to confusion that undercuts the standards process just as much as too little competition can create an unfair marketplace. Too many initiatives detract from those that have the most technical merit, creating confusion that eventually works against the interests of the vendors developing all the competing standards.

Leadership and consensus within the standards organizations themselves is also very important – particularly from the largest vendors. At the same time, this weight can be brought to bear unfairly on the process, and in some places can effectively undermine key initiatives. A standard committee that may be making good progress can suddenly find itself floundering if a key vendor pulls out of the process, even if the standard itself holds significant positive potential for the community at large.

Consensus is important, but at what cost? Standards epitomize the traditional academic approach to develop consensus around key topics. At the same time, they can also represent all that is wrong with using academic processes in corporate settings. Bureaucracy and long development cycles descend directly from the need to develop an adequate degree of consensus around all aspects of a standard, including the challenges in getting reference platforms implemented. Standards organizations would benefit from finding ways to dramatically lower time to market while maintaining process integrity.

Standards are too important to be allowed to continue in a dysfunctional and disengaged manner. It is time for customers and key organizations to step in and right the course, and perhaps help get the security and IT industries back on track in the process.

About the Author

Benjamin Tomhave, CISSP, is an independent consultant in Phoenix, AZ. He holds a MS in Information Security Management from George Washington University and is a member of committees within the American Bar Association and OASIS. He may be reached at tomhave@secureconsulting.net.