

Tag, Your IT!

ISO Software Tag Standards Come of Age



ITAK Columnist

Steve Klos

IAITAM Fellow,

Convener the ISO/IEC 19770-2:2009,

Executive Director of TagVault.org

Co-Founder of Agnitio Advisors

Software Identification tagging is receiving a significant amount of market attention lately. This attention has been coming from software publishers, tool providers and software purchasing organizations.

The standard defining software tags, ISO/IEC 19770-2:2009 was published by ISO with the final date on the document being November 15, 2009. The standard, as well as the XSD used by the standard are now finalized and will only be updated once the standard goes through its systematic review cycle (this needs to be done in 5 years). Organizations can now purchase the standard from ISO (available from the [ISO](#), [ANSI](#), your country's standards body, or even amazon.com) and all organizations can start developing and deploying or using software identification tags in their products today.

As software identification tags (SWID tags) roll out, they will lower the overall cost of implementation of effective and accurate software asset management (SAM) programs, while providing significant added value to an organizations operational security model. Cost savings will be recognized by all members of the SAM ecosystem from the publisher, to tool and service provider to the software purchaser. Organizations working with TagVault.org to ensure these changes happen include software publishers such as Symantec and CA, SAM Tool providers such as Express Metrix and ManageSoft, and end-user organizations such as the U.S. General Services

Administration (GSA).

TagVault.org is the certification authority for SWID tags. TagVault.org is a non-profit program of IEEE-ISTO and with the standard published, it has been making great strides to ensure the market has the tools, technology and information available to create, digitally sign and use software tags. TagVault.org is also specifying the certification requirements to ensure a rapid and consistent utilization of the variety of element data values SWID tags support. The overall goal of TagVault.org is to ensure the initial implementation of SWID tags is done as smoothly, quickly and at the least cost possible for all members of the software market.

Other than the fact that the standard has been published and is available for purchase, the other very big news in the SWID tagging environment is that the GSA recognizes the value that SWID tags will have on their work to create and standardize on an ITAM program for the U.S. Federal Government. The GSA has signed up as a member of TagVault.org and Alan Vander Mallie was quoted in a [press release that was distributed the week of December 7](#) saying the following:

“Certified software identification tags have the ability to dramatically increase the visibility of IT assets government-wide, while increasing security and operational efficiencies, and reducing the costs of government ITAM operations”, said Alan Vander Mallie, Federal ITAM Program

Manager of GSA. “The GSA program is looking forward to seeing software tags in use by all software vendors as soon as possible and is looking for federal agencies to share their tagging requirements. In the context of open and transparent Government, an organization such as TagVault.org allows federal agencies to participate directly with industry towards the common goal of increasing the compliancy and security of its assets. Software tagging efforts and the open exchange of tagging requirements support the basic tenets of the GSA IT asset management program (www.gsa.gov/feditam): know what you have and who you are buying from, manage and buy smarter, while increasing the overall compliancy of your IT assets”.

The goals of the Federal ITAM Program are not any different from the goals of an ITAM program at any large enterprise. The Federal Government typically has a much, much larger scale of problem than most enterprises. However, Government programs have all the same SAM and ITAM issues including:

- **Planning** – just like an enterprise, the Federal Government needs to know what it has, plan for what it needs and budget for those requirements – this includes the planning of software requirements.
- **Compliance** – the Federal Government has similar audit clauses as any enterprise – they can and do get audited if a software publisher believes they are well out of compliance. As mentioned, the scale of compliance issues is significantly larger, hence the need to leverage international standards and certification authorities which increase the benefits while decreasing the costs involved.
- **Security** – The Federal Government arguably has as many, if not more security issues to contend with when it comes to software installations. To support a secure environment, agencies must validate that the

correct individuals have authorized and properly identified software installed, and do not have unauthorized software installed.

- **Asset Optimization** – each agency has a fixed budget it needs to work within. Although portions of the government do, in fact, print money, that doesn't mean that any agency has an unlimited budget. Where software can be re-used, or maintenance contracts can be reduced, this helps ease the pressure of other expenses the agency must deal with.

Is it any wonder why the Federal Government is working to determine how certified tags can help to make the management of these issues more accurate while also reducing the costs involved in their management?

Adobe is one software publisher that immediately recognized the value that SWID tags would have to the whole ecosystem and started developing tags using their own engineering resources even before the ISO/IEC 19770-2:2009 standard had gone through its final reviews. Adobe's tags are not digitally signed, nor are they fully conforming to the published ISO standard, however, they are included in all CS4 products and they provide exact details about which product is installed and if the installed product is part of a suite or not. For CS4 products and later, customers, tool and service providers and Adobe (or any of Adobe's agents) can accurately identify if an Adobe product is installed as a standalone product, or as part of a suite.

Adobe's SWID tags will be helpful for organizations that have effective desktop management and SAM programs, but may be a concern for organizations that do not have effective programs. No longer, can organizations install a version of one Adobe CS4 application using a suite's product code on a computer and expect that in an audit situation that installation will be grouped with standalone Adobe products. If a product is installed using a product code for a suite, a

corresponding license entitlement for that suite must also be available in order to properly reconcile Adobe's software entitlements. Looking at a worst case scenario, if Adobe Acrobat version 9 (list price \$449) is installed using a product code for the CS4 Master Collection Suite (\$2,499), than during an audit that one installation could cost \$2,000 more than an organization may expect. It's unclear if Adobe will apply a strict interpretation to the software installations in this manner, but the point is that everyone who has access to the computer with this installation now has the ability to know if Acrobat Version 9 was installed, or if the Master Collection Suite was installed.

What does this mean for organizations that are doing a good job of discovery and working to ensure their licenses reconcile properly? It means that your discovery tool had better be pulling information from the SWID tags to identify the software. If the discovery tools are not doing this and are basing their reports on the old way of doing inventory reconciliation, and your organization does end up in an audit situation, there could be a significant finding that could cost the organization a lot of money! End-users who have automated inventory and discovery tools in place now had better be working with their tool providers to validate when those tools will be collecting and using Adobe SWID tags and how they plan on supporting fully certified SWID tags.

Adobe has also recognized that they need to provide details to the end-user and tool community on how to discovery and use their software tags. To this end, they have posted a blog entry that provides this detail - http://blogs.adobe.com/OOBE/2009/11/software_tagging_in_adobe_prod_1.htm. If your organization has Adobe CS4 software installed, it would be worthwhile reviewing this blog post and talking with your discovery or inventory tool provider!

What is a TagVault.org Certified software identification tag (Certified SWID tag)?



A TagVault.org certified SWID tag ensures that the tag conforms to the ISO/IEC 19770-2:2009 specification. Essentially, this means that the tag must have all 7 mandatory elements included. Beyond that, the certification provides a few more checks and balances that could not be written into the specification, but can be applied by a certification authority. These include:

- **Ensuring registration of values**
All data values used in the certified SWID tag such as regid must be registered with the certification authority. What this does is ensure that organizations will see a consistent and common set of regids used in every software tag from the same vendor, regardless of the group that created the software.
- **Ensuring normalization of data element values**
All optional elements that can have different values applied to them will be normalized. This ensures for example, that when a SAM practitioner wants to find all software products that installed in a "trial" state that they have only one value

they need to look for in the data element “activation_status” and they don’t have to guess at what other terms may have been used such as demo, trialware, sample, test, eval, evaluation, etc.

- **Secure validation of the publisher and specified data**

Certified SWID tags are digitally signed using a TagVault.org certificate that was subsequently signed by VeriSign. Any signed element can be validated that it did, in fact, come from the entity specified in the regid values and that the data has not been modified in any way since the publisher distributed it. This validation process can be done by any tool and does not require access to anything other than the tag data.

Additional benefits provided by TagVault.org for digitally signed tags include the following:

- **Secure validation of associated files**

Certified SWID tags that include a signature on the package footprint, security validation can apply all the way down to the file level. This means that inventory and discovery tools that capture individual files can reliably use this information to filter out all known “good” files that are associated with certified SWID tags and they will be left with only the files not specified in any SWID tag. Since organizations can make their own SWID tags and/or use SWID tags from other organizations, it is very straight-forward for an organization to get to a stable situation where the only unknown files are those that are coming from rogue, or unknown software. This allows an organization to focus much more reliably on a management by exception process rather than a management of every single item found process.

- **No time constraints applied to signatures**

The W3C recommendation utilized in the 19770-2:2009 standard does not explicitly specify how timestamps should be applied to a digital

signature. Since digital certificates used for signatures are only good for a specified period of time (typically one or two years), without a timestamp, the digital signature would need to be re-applied after the certificate expired. TagVault.org has created a tool (available in Beta form now), that applies timestamps in a manner that conforms to the ISO/IEC 19770-2:2009 standard as well as the W3C recommendation that specifies how digital signatures can be applied. This timestamp process is now being recommended to W3C for inclusion in their review of the recommendation and will be incorporated into the ISO/IEC 19770-2:2009 standard as a technical note and into the document itself when it goes through the review process.

All of this should be seen as very good news for anyone in the SAM or device management market who needs to deal with software identification. Certified SWID tags provide a way to do this in an authoritative and secure fashion while also getting access to tools, source code and documentation that will make the process faster, less expensive and ensure data values are normalized for all users. Symantec has already received the first official SWID tag to go through certification and we’ll announce when that product hits the market. Adobe has already started to release SWID tags and though they do not yet conform to the standard, Adobe has committed to ensuring that future SWID tags do conform.

What can software purchasers do to help?

All companies that buy and use software are required to agree to audit clauses in the software contracts. When renegotiating maintenance contracts, larger organizations (like the GSA, or any Fortune 1000 company) have the ability to strongly influence the priorities of software publishers by negotiating certain requirements and potentially delaying purchases, or even doing a more in-depth review of competing

products. If the software publisher includes an audit clause that they provide at least the information to you, as a purchaser, require the publisher to accurately identify installed software. Make sure your software vendor knows that if they expect to continue to include the audit clause in their software entitlements, that you expect them to provide a certified software tag as part of their software installation.

When writing RFP’s, ensure that you add a line item to know when certified software identification tags will be supported, or if they are already supported.

If security is an issue for your organization, it may make sense to request further details on the certified software tags and validate that the package footprint is included. This allows device management systems to automatically identify and validate software identification down to the file level of detail.

Be aware that any organization can develop SWID tags. The only tags that will be certified will be software publishers who’ve submitted their tags through TagVault.org. However, end-user organizations can utilize the TagVault.org tag creation and signing utility (available to all members above the adopter level) to create tags for individual products or even for system images and use these details to help move your SAM program from a firefight to a system that manages exceptions.