SAE International

Traceability in the Age of Globalization: A Proposal for a Marking Protocol to Assure Authenticity of Electronic Parts

2012-01-2104
Published
10/22/2012

Mitchell Miller, Janice Meraglia and James Hayward
Applied DNA Sciences Inc.

doi:10.4271/2012-01-2104

ABSTRACT

Proposes adoption of an industry standard marking protocol to assure the authenticity of high-reliability electronics. The protocol is seen as a key ingredient in the industry's effort to control counterfeit electronic parts escapes.

The specifications of the marking protocol have been informed by the experience of the authors, who are currently participating in a DNA marking program mandated by the Defense Logistics Agency.

The protocol would set out these criteria for an effective marking program:

- Simplicity
- Proven uncopyability
- Reportability: transparency and ease of oversight
- Legal validity: empowering of law enforcement
- Quick ramp-up and seamless implementation
- Extreme fidelity and absolute character of results - reliability of the mark at a very high level
- Universal adoption

INTRODUCTION

In this paper we urge adoption of a standard marking protocol which would assure the authenticity of high-reliability electronics. We see the protocol as a key ingredient in the effort to control the flood of counterfeit electronic parts into the industrial supply, a step that can weave together and optimize existing anti-counterfeiting standards.

The specifications of the marking protocol are informed by the experience of the authors, who are currently participating in a DNA marking program mandated by the Defense Logistics Agency.

The contours of the protocol would be straightforward: we urge the application of a mark at the unit level, that is, on each electronic part. The mark would carry information detailing the origin of manufacture, a date range, and perhaps other identifying data, and would be robust enough to travel and survive the entire length of any supply chain. Additional marks may also be added after parts integration to verify the builder or distributer.

The mark should be readable at any point along the supply chain using forensic methods to assure authenticity, and to provide an audit trail and legal validity.

SEARCHING FOR TRACEABILITY IN THE AGE OF GLOBALIZATION

Traceability has long been the Rosetta Stone in the effort to stem the tide of counterfeit electronics. It plays a central role in the SAE Aerospace AS5553 Standard - Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition, which states that organizations should require their suppliers to trace parts back to Original Chip Manufacturers (OCMs) in order to prove authenticity. The word figures early and prominently in Section 818, of the FY '12 National Defense Authorization Act (FY' 12 NDAA), the sweeping and seminal new legal requirements for defense contractors who provide electronics to the military.[1]

Yet at this point, *traceability* has been undermined to such an extent that many in the industry seemingly despair of any near-term or even long-term success with it. The ability to trace to origin in electronics has been undermined in part by

the burgeoning counterfeiting black market which has become increasingly capable of deceiving, avoiding, and simply overwhelming our ability to authenticate parts. But more powerfully still, traceability has been obscured by the steady globalization of the industrial base. The electronics supply chain, globalized, has been engulfed by a multiplicity of legal and accounting systems, differing cultures and national interests, and a very high degree of complexity. Entropy favors the counterfeiter, making it difficult to accurately monitor parts through chaotic supply webs that strongly resist efforts to trace parts.[2] These supply webs have become strikingly opaque, especially when not all participants are incentivized to exert controls.

There is no single solution to the problem, and this paper does not pretend to offer one. But we do believe that the effort can be cut down to size and having done so, the process of integrating standards, processes, and technologies can begin. We believe that adoption of a standard marking technology for high-reliability electronics is in line with that approach. The requirement to apply a unique mark, or tag, denoting source of each electronic part is certainly not new, but it can be, and has been, an effective form of authentication *if* it conforms to a robust set of requirements.

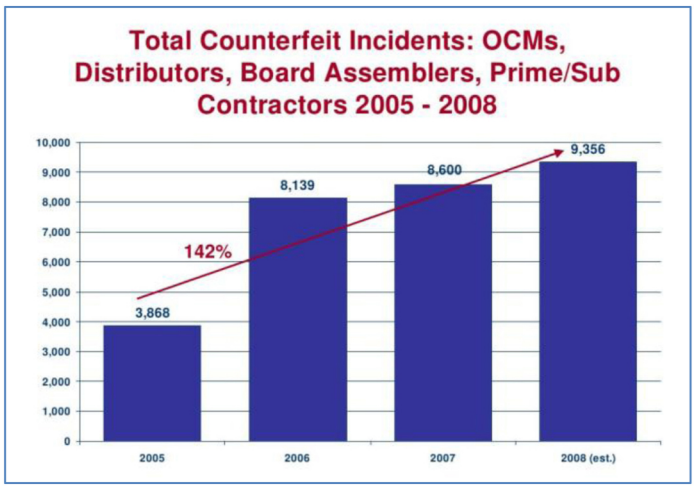

Figure 1. US Department of Commerce, Office of Technology Evaluation, "Counterfeit Electronics Survey," August, 2009

LESS THERE THAN MEETS THE EYE: HAVE WE REACHED THE LIMITS OF VISUAL IDENTIFICATION?

To date, visual inspection has been the front line of anti-counterfeiting measures, industry-wide, as it must. The IDEA-STD-1010A standard, developed by the Independent Distributors of Electronics Association is largely a visual inspection guide, all the more important because it is used by independent distributors, properly concerned about vulnerability in their channel. Some independents and others have raised the ante, adding de-capsulation, X-ray fluorescence, acoustic and other advanced microscopy and other technologies and processes.

Judging by outcomes, especially the spike in reported counterfeit incidents from roughly 2006 to date, the effect of the inspection standards has been uneven. (See Figure 1). (It should be added that the rise in reported incidents is even more startling when using a metric that compares counterfeit escapes as a percentage of shipments. This percentage has continued to rise sharply even through the worst of the recession beginning in late 2007 when shipments of microcircuits, for example, dropped as an absolute number, but the percentage of reported incidents as compared to shipments continued to rise, indeed at a somewhat steeper slope).

It is true that those distributors and others using rigorous testing based on advanced techniques have garnered a well-deserved reputation for effectiveness. But the adoption rate has been slow, as the capital costs and skill sets required are high indeed.

Visual inspection has become a strike/counterstrike race with the counterfeiters. Tom Sharpe, Vice-President of the independent distributor SMT, told the Senate Armed Services Committee on November 8 of last year: "The counterfeiters are most certainly monitoring our level of detection expertise and quickly evolving newer processes to introduce into the global supply chains. Many of the current counterfeit techniques are already beyond the in-house capabilities of most open-market suppliers."[3] Sharpe should know: in 2010 he embarked on a trip to Shantou, China, in an effort to follow the route of counterfeit parts through the global supply network.

Several factors are at play. First, the sheer volumes of counterfeits have become a problem, threatening to overwhelm traditional inspection methods. "You can't test every single part," says John Brown, of Verical, Inc., cited in Purchasing magazine. "Maybe you test 10 in 1,000." [4] But spot-checking, the only reasonable approach to inspections, is of scant comfort when even a single counterfeit part escapes and finds its way to an operational computer for a defensive missile system.

Then there are the increasingly more subtle measures taken by counterfeiters to defeat inspection. For example, many plastic-packaged integrated circuits are manufactured with cavities purposefully created during the mold process. Most commonly, these look like round indents on the surface of the IC. The idea is that blacktopping, the well-known counterfeiting technique, will fill those cavities and tip off the inspector who, using documentation of the chip structure,

knows an indent should be there. Now, however, counterfeiters are creating faux indents after blacktopping. (See the American Electronic Resource backgrounder "Detection of Counterfeit Electronic Components" for further detail.)[5]

Says Paul Romana, of Fusion Trade:[6] "…the task of ensuring authenticity is becoming increasingly tricky as counterfeiters become more and more savvy. No longer will a visual inspection cut it."

All this should cast some light on the controversy surrounding redaction of photos taken by the U.S. Customs and Border Protection agency (CPB) in their port and border inspections of imported electronics. There are many who call for an end to the practice of redaction, while the CPB, which is concerned that a Port Officer may be liable to arrest and prosecution under the Trade Secrets Act, currently defends the practice.[7] Our point is simply that imaging alone, accompanied by no other techniques or technologies cannot possibly be more effective then on-site visual inspection, and that, as we have seen, is presently limited.

By contrast, one can readily see the advantages of a robust, uncopyable mark. The technique relies on the simplicity of a single durable mark which is not subject to the strike/ counterstrike duel with the counterfeiters. It is scalable in a way that intensive inspection procedures and costly advanced tools can never be.

What's more, the mark would meld nicely with existing inspection and other measures. Used as a screen, mark detection can aid in isolating "hot zones," where suspicion and risk of counterfeits appears to be high. Used as a backstop, an uncopyable mark and authentication protocol add a forensic and absolute identification process. In both circumstances, a mark-and-authentication ingredient can reinvigorate conventional inspection methods.

THE THREAT TO FAILURE ANALYSIS AND THE ISSUE OF DESTRUCTIVE TESTING

Self-evidently, authentication techniques, such as a mark-and-authentication protocol, cannot take the place of failure analysis and defect tracking. Root cause analysis and the rich data which accrue will always be bedrock of an integrated approach to anti-counterfeiting strategies. But FA is not intended as a screening tool, and yet as we learn anecdotally, the FA community has found itself preoccupied with a wave of counterfeits. While counterfeits may very well be defective of course, or non-conforming to spec, or outright non-functioning, that discovery adds little to a manufacturer's QC. This problem can be strongly mitigated by a screening standard, such as an uncopyable mark.

Failure analysis, including against suspected counterfeits, can add immeasurably to our understanding of counterfeiting techniques, trend lines, sourcing, and to the effectiveness of our own monitoring and reporting. However, by their nature, FA techniques are intensive, and sometimes destructive; that community should not be placed de facto, as a front-line screen against counterfeits.

TOO CRITICAL TO FAIL: THE RISE OF ZERO TOLERANCE ELECTRONICS

As consumers, we are often delighted with the wonder of, say, an iPad. We may be entranced by what sometimes seems to be the digitization of everything, and we are comforted by the safety and protection which advanced electronics has offered in medicine and to our military. Less obvious, except in a crisis, is our dependence on electronics in certain areas, and the great risks which result. In a system charged with intercepting incoming ballistic missiles, for example, electronics failure is not an option. The same is clearly true for some medical devices, aircraft; more broadly high reliability and critical safety parts.

We may call this "zero tolerance" electronics, applying the term to both functionality and to supporting supply systems. We refer here to the semiconductors, the discrete parts, the boards, which absolutely must be authentic; where risky parts, including counterfeits, cannot be allowed to pass through a simple spot check. If centralization in our financial system has aided the rise of banks too big to fail, our infrastructure has seen the advent of electronics too critical to fail.

Here the need for an integrated and standardized approach to anti-counterfeiting is most clear and most immediate. In this area, an uncopyable mark, functioning both as a screen and as a forensic backstop, is clearly a key ingredient.

Here we can see also some practical advantages of a marking protocol. In zero tolerance electronics, we have a true crisis where quick ramp up of new tools and procedures is urgent. Only a tested and simple tool can meet the need for speed in such a crisis. In this connection, an uncopyable mark, and associated authentication process for that mark, has already been tested by our own company in a project supported by the Defense Logistics Agency. This experience has also taught us that any marking and authentication system must, realistically, be capable of folding into an existing production process with little friction.

Finally here, we would suggest exploration of the marking initiatives enforcing the RoHS and WEEE directives regarding hazardous substances such as lead in electronics. While controversial in some ways, the marking initiative by

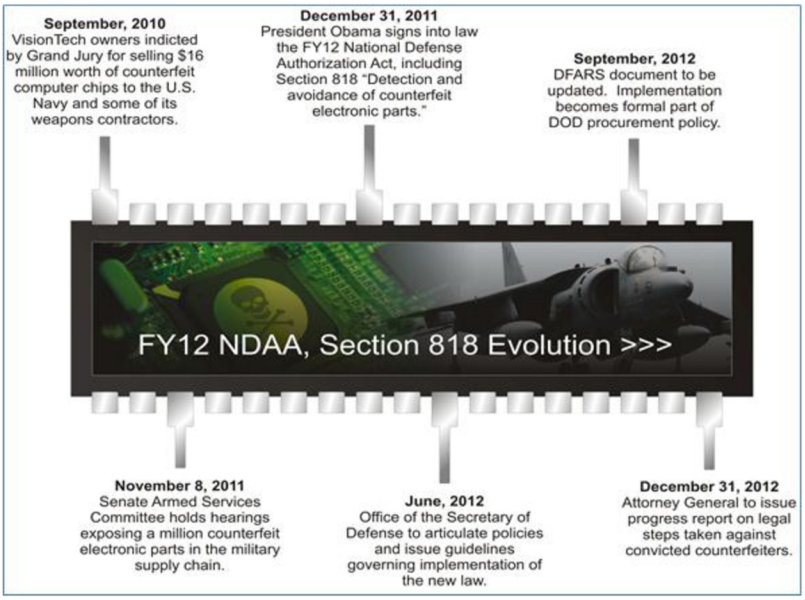

Figure 2. Timeline, Section 818 of the National Defense Authorization Act for Fiscal Year 2012. Graphic: Applied DNA Sciences, 2012

the EU may provide useful and on the whole successful experience with a marking protocol.

CRIME PAYS? THE EASE OF COUNTERFEITING

Within the electronics business, our efforts against counterfeiting must focus on the industry itself; it is what we can control. However, to state the obvious, there are real criminals involved in the counterfeiting trade, and we do have a responsibility and self-interest in putting them out of business and behind bars, where they belong.

The profits from counterfeiting and illicit goods are often compared to those from illegal drugs.[1] It is a lucrative business, and one populated by bad actors, some of whom may have motives more sinister than greed alone. With the investigation and 2010 convictions in the case against the counterfeit purveyor VisionTech by the U.S. Justice Department, the feds seem to be sending a signal that the joy ride is over: the consequences for proven counterfeiting, especially those sold to the military, will be harsh.

Similarly, Section 818 of the FY '12 National Defense Authorization Act imposes major fines and jail terms for convicted criminals in this area, and requires the Attorney General to report on enforcement progress at the end of 2012. (Figure 2.)

This being the case, the legal validity of our authentication process in electronics…matters. A mark, in our view, must be not only uncopyable and absolute in character, but must hold up in court. A forensic test of the identity of an electronic part must have the same legal standing as, say, the DNA-based identity findings in a criminal trial. Nothing less will empower law enforcement.

A PROFUSION OF ANTI-COUNTERFEITING STANDARDS

It is to the credit of electronics industry associations that an array of anti-counterfeiting standards has proliferated. This has been especially true in our view since the eye-opening studies by the Department of Commerce Office of Technology Evaluation in 2008 and 2010 and to ground-breaking work by figures in the industry such as Henry Livingston, Gary Shade, Bhanu Sood, Jack Stradley, and others. The roles of the SAE AS5553 Standard, the IDEA-1010 standard and others are still playing out.

It is our opinion that a new, implicit, contractual Standard of Care for electronics-aimed at preventing counterfeits from entering the military supply chain-may be indicated in Section 818, of the FY'12 NDAA. This too would represent a new standard for the industry.

---

[1] Union des Fabricants pour la Protection Internationale de la Propriete Industrielle et Artistique, "Counterfeiting and Organized Crime," p. 9. "According to Detective Superintendent Alain Defer, …, "the profits are similar to drugs trafficking, about €10 per euro invested (…) In France, selling counterfeit products is punishable by a two-year prison term and a €150,000 fine, while selling drugs is punishable by a ten-year prison term and a €7,500,000 fine. According to Jorn Rise Andersen, chairman of the Danish customs and excise association, "counterfeiting brings in more money than drugs trafficking and it's less risky".

Important as these protocols may be, all necessarily tend to be process-based and procedural, lacking the heart and soul of a practical technology. In short, we have passed through a stage of developing standards. We need now a catalyzing event to integrate and activate them.[2]

We believe the universal adoption of an uncopyable mark to prove origin of electronics could be that event.

HOW DO WE KNOW WHEN WE ARE SUCCESSFUL?

Every project manager is ready with his or her metrics. We do not want to succeed invisibly-we want our sponsors and peer group to know how to judge our success. If we fail, we want to learn the lessons and recover. Somehow we have missed this step in the greater, macro picture of anti-counterfeiting in electronics. We advocate an array of solutions-many which may surely be integrated into a greater effort-but we make no promises. Thus we offer no way to gauge progress, and no motivator to those who would benefit and therefore fund us-customers, taxpayers, the corporate center.

At the very least, an authenticating mark, if adopted widely, gives us the basis to report progress. Use of the mark as a screen, and also as a forensic backstop, each represents discrete, measurable events, recorded digitally, and available for oversight. This gives us, at least, measurable data.

One obstacle to developing a metric has been that counterfeit incidents are severely under-reported. The OTE in a 2009 study found that less than half-49% -of organizations encountering counterfeit electronics reported them, and far fewer communicated to the government's formal reporting channel, the Government-Industry Data Exchange Program (GIDEP) database; about 14% for all participants.[8]

While an authenticating mark is certainly not the only tool which would provide a new, clean metric, it does fill that bill. For example, in a comparison of screened suspects to lab-confirmed counterfeits, one might expect the confirmation rate to improve long term, as counterfeits are flushed out of the system.

UNIVERSAL ADOPTION

In January, 2010, the Department of Commerce, Office of Technology Evaluation (OTE) published a now famous study commissioned by the Naval Air Systems Command (NAVAIR). According to Phil Zulueta, Chairman of the SAE G-19 Committee, the study was commissioned because "NAVAIR suspected that an increasing number of counterfeit/defective electronics were infiltrating the DoD supply chain and *affecting weapon system reliability*." (Our emphasis).

Zulueta calls our attention to "General Findings" of the OTE, nearly all of which, alarmingly, pinpoint lack of communication, reporting, and accountability, reflecting the lack of a universal system or standard.

The findings were:

- All elements of the supply chain have been directly impacted by counterfeit electronics;
- There is a lack of dialogue between all organizations in the U.S. supply chain;
- Companies and organizations assume that others in the supply chain are testing parts;
- Lack of traceability in the supply chain is commonplace;
- There is an insufficient chain of accountability within organizations;
- Recordkeeping on counterfeit incidents by organizations is very limited;
- Most organizations do not know who to contact in the U.S. Government regarding counterfeit parts;
- Stricter testing protocols and quality control practices for inventories are required;
- Most DOD organizations do not have policies in place to prevent counterfeit parts from infiltrating their supply chain. [9]

We can allow ourselves some dismay at this. But the reasons are not so hard to understand. The approaches we have now, mainly process-based and procedural, do not scale. They are intensive programs packed with extensive hiring, department re-engineering, and training. As for reporting, there has been little incentive to do so, and more than a few disincentives working in the opposite direction.

But we believe those conditions are about to change. If Section 818 FY′12 NDAA is implemented as it is worded today, timely and consistent reporting provides a safe harbor from legal consequences of inadvertent counterfeit escapes when providing electronics to the military. This is a powerful motivator indeed. And we believe, with others, that the new law will have widespread impact over the "entire defense industrial base," in the words of the Council of Defense Space and Industry Associations. [10]

The time is ripe to adopt a practical standard, such as marking to origin, which gives the industry a ready-made, relatively

---

[2] We mention here a separate impediment to anti-counterfeit action by the industry: we have been hamstrung by wrangling over a formal and legal definition of counterfeiting. That definition is far from trivial and has real business and legal import, but it is past time to put it aside in favor of a workable action plan.

frictionless, relatively cost effective, route to compliance. This route will differ somewhat, or greatly, according to the stakeholder. However, we believe that a marking standard, in part again because of its very simplicity, can be designed to satisfy the various needs of OCMs, OEMs, authorized distributors, independent distributors, brokers, federal oversight and procurement agencies, and law enforcement.

WHAT KIND OF MARK THEN?

Flatly, the success of a marking standard rests on the quality of the mark. Our industry is replete with examples of insecure marks and labeling, unprotected 2D bar codes, taggants and the like. The mark we have in mind is one of extreme fidelity and is characterized by the absolute character of its results. This criterion would set the bar very high, insisting on the reliability of the mark at a very high level.

This mark must be uncopyable-in a best practices environment it must be virtually impossible to back-engineer and reproduce them and must have very high fidelity. Granted, enormous resources would be hurled into breaking and reproducing the mark. It may even be right to caution ourselves to "never say never." But we believe this goal is within our grasp, and we must try.

A special word about electronic taggants, a form of marking which we believe does not satisfy the requirements for a universal form of electronics authentication, and especially not for semiconductors, a major counterfeiting target. In some environments, and at a specific stage, taggants can provide a unique code or fingerprint to authenticate originality. However, as evidentiary tools, the value of a taggant only increases as a function of the density of its information content. This density is presently too great to be effectively deployed at semiconductor scale.

Mineral taggants, which simply provide parameters of chemical identity and concentration, are only effective as rapid screening tools, often by handheld detectors. Stochastic arrays of fibers or particles are difficult to incorporate in the media used to fabricate microchips and semiconductors. Stochastic arrays of nanoparticulate ferrite can generate complex "fingerprint" patterns, but care must be exercised to ensure the magnetic field does not interfere with semiconductor function.

CONCLUSION

It seems to us that the EEE space has passed from a phase of shock and awe as the counterfeiting problem has forced itself on us, through a period of standards development and new procedural ideas. As an industry, we now await tools and a program to integrate and activate these standards. We advocate one such tool here: a marking system that allows absolute and robust proof of origin and offers, in a word assured authenticity.

We believe that such a standard for marking to origin for high reliability electronics is possible and necessary; more, it is the order of the day. Success depends first and foremost on the quality of the mark, especially its absolute resistance to malicious back-engineering and reproduction. The mark itself must not be counterfeited. There are those who say that may not be possible, but we think we can demonstrate that it is. In a more visionary sense, if our defense industrial base can produce ballistic missiles which can intercept others in mid-flight, surely we can accomplish this.

REFERENCES

1. U.S. House of Representatives, "NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2012, CONFERENCE REPORT TO ACCOMPANY H.R. 1540," p. 198 cf : "…guidance shall address requirements for training personnel, making sourcing decisions, ensuring traceability of parts…"

2. Much is owed to the seminal paper by Shade, Gary, and Sood, Bhanu, "The Perfect Storm, Now appearing in FA Labs Everywhere," paper delivered at the Center for Advanced Life Cycle Engineering (CALCE), University of Maryland, College Park, MD, p 2 ff.

3. Senate Hearing 112-340, "THE COMMITTEE'S INVESTIGATION INTO COUNTERFEIT ELECTRONIC PARTS IN THE DEPARTMENT OF DEFENSE SUPPLY CHAIN," November 8, 2011

4. In Purchasing, "Strategic Sourcing," September 2009, p. 24E10

5. American Electronic Resource Association, "Detection of Counterfeit Electronic Components, undated

6. Romano, Paul, "Counterfeit Parts are on the Rise," Embedded Intel Solutions, http://www.embeddedintel.com/special_features.php?article=1496

7. For further discussion, see Livingston, Henry, "NDAA SEC 818(G) AND EXPECTATIONS TO STOP COUNTERFEITS AT THE BORDER," March 4, 2012, http://counterfeitparts.wordpress.com/2012/03/04/ndaa-sec-818g-and-expectations-to-stop-counterfeits-at-the-border/ "For the past three years, the Semiconductor Industry Association (SIA) Anti-Counterfeiting Task Force (ACTF) has been working to fix a dispute over Customs and Boarder Protection (CPB) redaction policy by pursuing legislation to include specific authorization for CPB to return to its pre-2008 practice of sharing unredacted photos of suspicious chips when they are identified at ports of entry. The particulars of this issue are described in SIA's 7 July 2011 testimony before the House Committee on Homeland Security Subcommittee on Oversight, Investigations and Management."

8. US Department of Commerce, Office of Technology Evaluation, "Counterfeit Electronics Survey," August, 2009.

9. Zulueta, PhilChairman, SAE International G-19 Counterfeit Electronic Components Committee, "Are you Prepared for HR 1540: National Defense Authorization Act for Fiscal Year 2012, (Sec. 818, Detection and Avoidance of Electronic Parts), Slide 17

10. Council of Defense and Space Industry Association (CODSIA), Open Letter, "Subject: Implementation of Section 818, Detection and Avoidance of Counterfeit Electronic Parts, National Defense Authorization Act (NDAA) for Fiscal Year 2012, To: Mr. Richard T. Ginman, Director, Defense Procurement and Acquisition Policy, and Mr. Alan F. Estevez, Assistant Secretary for Logistics and Materiel Readiness (OUSD (AT&L))" February 21, 2012. http://counterfeitparts.wordpress.com/2012/02/24/codsia-letter-to-dod-re-implementation-of-section-818/

APPENDIX

APPENDIX A

Subsequent to the initial writing of this paper, the Defense Logistics Agency issued a notification to suppliers of microcircuits, requiring a DNA-based authentication mark, such as the one described in this paper, be applied to all parts falling into the federal classification FSC 5962 (microcircuits). The authors are participating in this program. We believe that the experience to be gained by the industry as the program moves ahead both validates and enriches the arguments here for an industry standard protocol. The wording of the notification, which appeared on the Defense Logistics Agency Internet Bulletin Board system on August 7, 2012, is repeated here for reference:

> *"DLA is implementing new requirements for deoxyribonucleic acid (DNA) authentication marking on items falling within Federal Supply Class (FSC) 5962, Electronic Microcircuits, which have been determined to be at high risk for counterfeiting. A new clause at Defense Logistics Acquisition Directive (DLAD) 52.211-9074, Deoxyribonucleic Acid (DNA) Marking on High Risk Items, will be included in new solicitations and contracts for FSC 5962 items when the item description states that the item requires DNA marking. The clause requires contractors to provide items that have been marked with botanically-generated DNA produced by Applied DNA Sciences or its authorized licensees, if any.*
>
> *"Contractors shall obtain the DNA marking material from Applied DNA sciences or an authorized licensee, and may contact them at militarymark@adnas.com. The DNA marking can be applied with an invisible DNA mark on the part, or the contractor's ink utilized for part marking can be mixed with the DNA marking material. The authentication DNA used shall be unique to the contractor. Contractors will be required to retain traceability documentation that demonstrates the items provided under the contract have been marked with DNA material produced by Applied DNA Sciences or an authorized licensee, and that the DNA marking is unique to the contractor. DLA is proceeding with this marking requirement for FSC 5962 in order to implement effective authentication marking while concurrently initiating a research and development effort to evaluate comparable DNA and alternative authentication technologies for intended application to all electronics items. A forthcoming Request for Information (RFI) will request input concerning authentication marking technologies that would satisfy DLA's requirements as outlined in the RFI.*

Posted 08/07/2012

The Engineering Meetings Board has approved this paper for publication. It has successfully completed SAE's peer review process under the supervision of the session organizer. This process requires a minimum of three (3) reviews by industry experts.

ISSN 0148-7191

SAE Customer Service:
Tel: 877-606-7323 (inside USA and Canada)
Tel: 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
SAE Web Address: http://www.sae.org
Printed in USA