DNA Marking and Authentication:
A unique, secure anti-counterfeiting program for the electronics industry

Applied DNA Sciences, Stony Brook, NY, USA
media@adnas.com

Introduction
DNA (deoxyribonucleic acid) is a form of forensic evidence trusted by law enforcement and recognized by international courts around the world. This abstract provides an introduction to the utility of botanical DNA taggants to provide supply chain security for electronic components and to protect against counterfeiting and diversion. A detailed treatment of the science behind Applied DNA Sciences' (APDN's) botanical DNA technology, its applications to semiconductors and microchips and an overview of DNA analysis by Polymerase Chain Reaction (PCR) and Cell Electrophoresis (CE) analysis is provided. In addition, we draw an outline of a marking and authentication program as it might be implemented in a microchip supply chain environment, as an indicator of its efficacy against current known counterfeiting strategies.

Counterfeit Electronics – A Global Threat
The evolution of product counterfeiting as a trade nearly parallels the evolution of technology itself. The last two decades have witnessed explosive growth of technology, and the condensation of travel, communication and the massive impact of the internet ensured these new technologies were laterally propagated instantly across the globe. Now counterfeits emerge on the market nearly simultaneously with new product launches, in time for the counterfeits to benefit from the marketing efforts expended by the original. The International Chamber of Commerce estimated in 2011 that the global economic and social impacts of counterfeiting and piracy will reach $1.7 trillion by 2015, representing between 5% to 7% of all world trade (Source: International Chamber of Commerce.)[1]. But this is more than a vexing nuisance for brand owners. Counterfeits threaten economies, destroy health and take lives, and destabilize the military.

The Defense Standardization Program Office (DSPO) Journal (Oct/Dec 2009) recognizes the definition of a counterfeit electronic part as "one whose identity or pedigree has been deliberately altered, misrepresented or offered as an authorized product." Early reports of counterfeit electronics emerged from industry. In May of 2006, The New York Times reported a massively coordinated effort of 18 factories in China to copy the entire product line of NEC. Nearly every aspect of the company's brand and product line had been replicated and sold along parallel paths. NEC even found itself honoring the warranties for the fakes.[2]

By June of 2007, the US Department of the Navy became increasingly convinced that a large number of counterfeit electronics had infiltrated the supply chain of the Department of Defense (DOD). In collaboration with the Department of Commerce (DOC), a study was initiated to assess the defense industrial supply base and to determine the statistical frequency of counterfeit electronics penetrating DOD. The results of this study, finalized in January, 2010 (US DOC "Defense Industrial Base Assessment: Counterfeit Electronics"[3]) showed:

- All elements of the military supply chain have been directly impacted by counterfeit electronics;
- Stricter testing protocols and quality practices are required; and,
- The use of counterfeit detection technologies by parts manufacturers, distributors and integrators should be expanded.

It seems that every opportunity to leverage the efforts of others is taken by counterfeiters. Both obsolete parts and current production are copied.

In the military supply chain a particular concern has been that the "noise" of counterfeit parts in the system might obscure efforts to identify more malicious and targeted infiltration of parts purpose-built to damage critical systems including weapons system—in short, sabotage by counterfeit.

Current Anti-Counterfeiting Measures are Inadequate
Current efforts to secure the authenticity of electronics are first attempted at the primary and secondary packaging stages. Traditional security platforms to prevent counterfeits are now also part of the counterfeiter's target and consequently within the retinue of counterfeiter's resources. New advances in holograms, optical strips and RFIDs are often available as near-perfect copies within days of their initial launch.
Exacerbating the inadequacy of packaging security solutions, most distributors and integrators store microchips and semiconductors in high-volume bins, capable of matching the demands on their supply. This "bin approach" excludes the secondary packaging to save space and time, so security must be implemented at the product level.

Product inspections offer decreasing value as a method of authentication. External visual inspections should no longer be used as a standalone authentication. Physicochemical characterizations are often destructive and rely on a degree of similarity to a bona fide original and the tolerance of the measurements.

Taggants can provide a unique code or fingerprint to authenticate originality. However, as evidentiary tools, the

value of a taggant increases as a function of the density of its information content. 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.

Forensic DNA foils and prevents all current counterfeiting strategies.
In contrast to present authentication technologies, DNA both foils and pre-empts counterfeiting strategies.

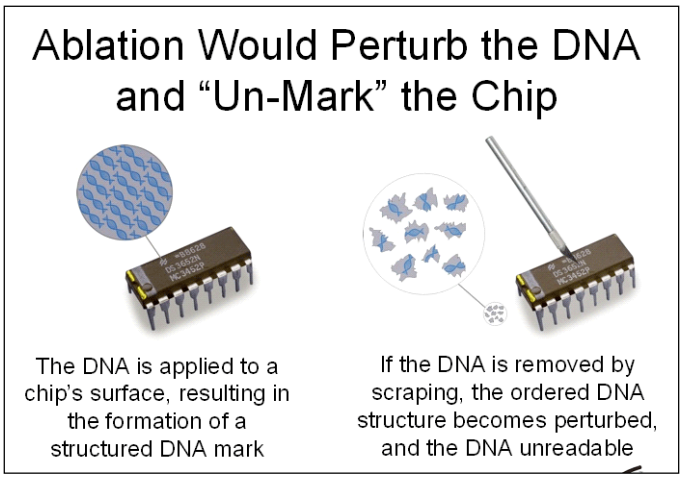
It ***foils*** counterfeiting strategies because it is uncopyable. Unlike even the most complex labeling, serialized code, etched or inked symbolization, even microdot application - all of which may be copied or sufficiently mimicked - DNA marks cannot be reproduced or simulated. Consider that DNA authentication, used by forensic laboratories all around the world, including the FBI, is absolute in character. When used to identify individuals or to establish paternity, the error frequency for false positives is less than one in a trillion.

DNA ***pre-empts*** counterfeiting because it is incorporated into the chip production process itself. Any ablation, sandblasting, blacktopping, or refurbishing of the chip will distort or remove the DNA mark, a sure tripwire within the authentication work flow.

Countering the fakery
Let us examine how these properties effectively safeguard against the major counterfeiting strategies today.

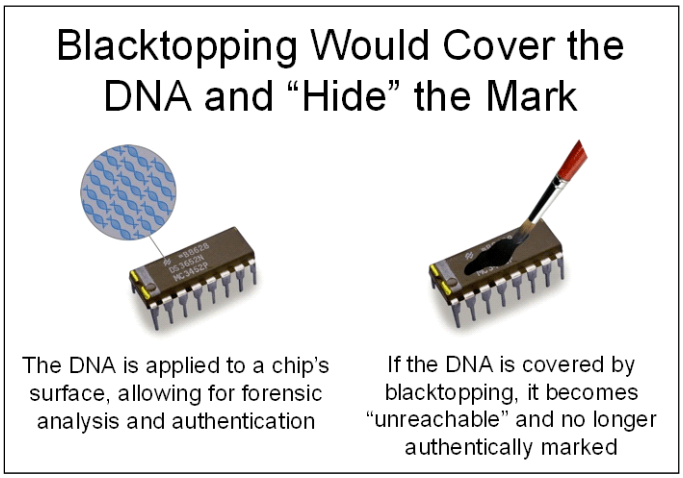
Sandblasting and other ablation (Figure 1) This technique would perturb the DNA and "un-mark" the chip. DNA is applied to a chip's surface, resulting in the formation of a structured DNA mark. If the DNA is removed by scraping, the ordered DNA structure becomes perturbed, and the DNA unreadable.

Figure 1



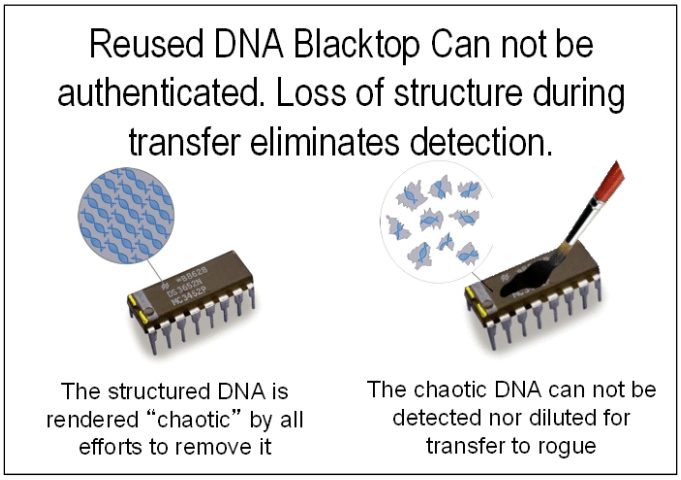
Blacktopping (Figure 2) Would cover the DNA and "hide" the mark. If the DNA is covered by blacktopping, it becomes "unreachable" and the chip is no longer authentically marked. It will not pass its authentication program.

Figure 2



Reused DNA Blacktop (Figure 3) Cannot be authenticated. Loss of structure during transfer disables the mark. It will not pass its authentication program.

Figure 3



Repackaging DNA is obscured even by partial repackaging. If repackaged, the DNA mark will not be detected, thus the chip will not pass an authentication program.

Forensic DNA as a High-Content, High-Resolution Taggant to Track Provenance and Ensure Authenticity
It is important to understand why DNA is unique and uncopyable in a way that no other form of encryption can match; why there is no better proof of identity**.** Evolved over eons, DNA provides the blueprint for all of biology. The information content is massive and highly customized by organism. With a capacity for content that is often compared

to computer machine code, DNA is a linear polymer of extraordinary molecular weight that stores its information as a sequence of infinitely variable organic bases.

However, unlike binary machine code, DNA's code is quaternary, storing its content as a linear array of four organic options for each bit. DNA has become the "Gold Standard of Forensics" due to its uncanny variability (consider all the variability across organisms and the variation within species), matched by a stringent fidelity, and detection methods that readily identify single molecules of a unique sequence (a detectability that will never be matched by any chemical or physical assay). Challenged by courts around the globe since 1980, there is no better proof of identity, nor is any better proof of identity likely to evolve.

Botanical SigNature® DNA:

- Is unequivocally uncopyable. This is the basis for its legal acceptance,
- Can be forensically authenticated when analyzed in the laboratory,
- Is detectable in the field,
- Will not require major changes in the manufacturing process
- Is chemically compatible in a wide range of security inks (overt and covert), varnishes, adhesives and substrates
- Is used as a taggant at extremely low concentrations
- Will not alter the quality of any carrier (such as ink, coatings, adhesives, plastics or commercial products)
- Persists, in physicochemical extremes such as harsh outdoor environments and high temperatures
- Can be elevate other anti-counterfeiting measures including barcodes, holograms, RFIDs, to a forensic level and
- Is an environmentally friendly, "green" technology derived from botanical DNA

Key Attributes of SigNature® DNA

Applied DNA has proven that its botanical DNA technology provides the following advantages over existing competitive security options.

- ***Resistant to reverse engineering or replication*.** The botanical SigNature® DNA platform is virtually impossible to copy. Proprietary methods yield DNA taggants so complex that they are statistically impossible to duplicate. In addition, the DNA segment used in the taggants needs to be replicated billions of times in order for detection and identification to take place, a process that can only be achieved by applying matching strands of DNA. Thus, the sequence of the relevant DNA in a specific taggant must be known in order to manufacture the primer needed for the detection process. The inability of counterfeiters to duplicate SigNature® DNA taggants has been proven in the marketplace.

- ***Proven.*** A European media manufacturer's production of millions of optical digital video discs (DVDs) in China included twelve anti-counterfeiting security platforms. Within nine months of the launch of the DVDs, 11 of those 12 anti-counterfeiting technologies themselves counterfeited and rendered ineffective, with SigNature® DNA being the only exception. Moreover, SigNature® DNA taggants on those DVDs remain effective to date, several years after launch.

- ***Secur****e*. Applied DNA maintains its records of DNA sequences which are held in a highly secure fashion on a cloud-based server. Sequences are encrypted, available to individuals on only a partial basis.

- ***Low Cost and High Accuracy.*** SigNature® DNA taggants are relatively inexpensive when compared to other anti-counterfeiting measures, such as RFIDs, integrated circuit chips, and holograms. The costs associated with the production of DNA taggants are not significant since the amount of DNA required for each taggant is small In addition, incorporating SigNature® DNA into products does not require major changes to the manufacturing process or logistic chain. The relatively low cost of SigNature® DNA does not affect its reliability. The probability of mistakenly identifying a SigNature® DNA taggant is less than one in a trillion, making it virtually impossible to wrongly identify something marked with SigNature® DNA.

- ***Easily Integrated with Other Anti-Counterfeit Technologies.*** SigNature® DNA taggants can be embedded into RFID devices, labels, serial numbers, holograms, and other marking systems using inks, threads, and other media. The Company believes that combined with other traditional methods, the SigNature® DNA solution provides a significant deterrent against counterfeiting, product diversion, piracy, fraud, and identity theft. In addition, SigNature® DNA would elevate these other methods to a forensic level. For example, in our experience with legal proceedings in cash robberies, DNA marks have been fully accepted by the courts.

- ***Broad Applicability.*** Applied DNA's ability to integrate taggants in a variety of ways allows SigNature® DNA technology to be embedded into almost any consumer product or item. SigNature® DNA taggants do not alter the quality of the product and are stable and long-lasting. In addition, as SigNature® DNA technology is safe to consume, it can be used in pharmaceutical drug tablets and capsules although that would naturally require FDA approval.

- ***Scalable.*** DNA taggants can be produced in essentially infinite variety. Individual taggants of defined sequence can be manufactured in large scale. For example, in a single batch APDN recently marked 500,000 lb. of raw cotton fibers before ginning. DNA-tagged, individual fibers could

be traced throughout the manufacturing process to the completion of retail garments and apparel.

IP and Trade Secrets:

APDN's intellectual property (patents and trade secrets) provide the mechanisms for protecting DNA in harsh chemical and physical environments (see Table 1), the insertion of DNA into plastics, films, adhesives, inks, metal surfaces, and protects the methods used to enable DNA to function as a commercial authentication tool.

Table 1: DNA MARKERS' STABILITY
Applied DNA Sciences, Inc.

Test	Test Specifics	Results
UV Energy	Equivalent to more than 350 years of UV energy accumulation in Denver	Stable
X-ray	4 times the X-ray exposure by scanning machine in an airport	Stable
y-Ray	30 kGy (kilo-Gray) radiation exposure by y-ray sterilization machine	Stable
pH	Exposed to pH of 1 to 14 overnight	Stable
Thermal	> 250 degrees Celsius (4 hours)	Stable
Solvents	Aggressive aprotic solvents, oxidizers, radicals	Stable

DNA for protection of Cash-and-Valuables-in-Transit (CViT), the Ultimate Arbiter of Secure Logistics
Since January 2008, Applied DNA has been working with Loomis UK, a cash-handling company that moves over £150 billion in cash annually. APDN has developed taggants in fixatives (the DNA remains in a fixed location) or in transferrable (the DNA may be transferred by iterative contact) formats. Applied DNA has successfully authenticated stolen bank notes, cash-and-valuables-in-transit (CViT), and other recovered evidence received from UK police forces, which is used to assist in the prosecution of the alleged criminals. The SigNature® DNA markers present in recovered evidence have resisted removal even after vigorous washing and have also been detected on personal items such as clothing and mobile phones belonging to the suspects in the investigations. Applied DNA has established a DNA Authentication Laboratory in Yorkshire, United Kingdom.

UK police departments have retained Applied DNA Sciences to assist with forensic authentication and the provision of expert witness statements. To date, forty criminal investigations in the UK, from eighteen different police forces have used SigNature® DNA taggants on recovered, stolen currency. These investigations have resulted in a 100% success rate in linking criminals to the crime. To date, more than twenty of these cases have progressed to conviction with cumulative sentences in excess of 120 years. [4]

All told, APDN's customers enjoyed a 49% reduction in losses as a result of CViT offenses year-to-year while the UK industry as a whole saw a decrease in losses of only 34%. Showing public support, the UK Police and Applied DNA earned the 2010 Sheriffs Award and the Guardian Public Service Award. Additionally, the Swedish National Police has begun using APDN's DNA taggants throughout its operations as a part of their crime fighting technologies.

SigNature® DNA botanical taggants cannot be copied or reverse engineered and have already been independently validated through a two-year vetting process conducted by the Department of Energy (DOE) and the Idaho National Laboratory. This technology has been selected as the sole anti-counterfeiting platform in a program funded by the European Regional Development Fund (a fund allocated by the European Union) and Yorkshire Forward. DNA applications will include the protection against counterfeiting and diversion of UK manufactured textiles from "fiber to fabric." Additionally, these taggants have been tremendously successful with law enforcement agencies across Europe resulting in criminal convictions and jail time.

Applied DNA Sciences Successfully Marks Mission-Critical Microchips for the Department of Defense
In 2011 APDN successfully completed a program to DNA mark microchips for the Defense Logistics Agency (DLA) an agency of the DOD.[5]

In this program, an original chip manufacturer (OCM) marked 100% of its production for a period of two months. The microchips themselves were scanned at the OCM facility, the DNA-marked outer packaging was scanned at a Distributor. In a blind sampling, where both marked and unmarked chips were sampled, forensic analysis confirmed the authenticity of products DNA-marked as genuine.

Results:
- 100% distinction was made between DNA-marked and unmarked product and packaging
- 100% forensic authentication of DNA-marked product and packaging
- No change was necessary to the production process
- No adverse impact to mark-permanency quality assurance test results at the OCM
- Marks were rapidly scanned without difficulty at both the OCM and the distributor
- Marking was non-destructive

The cure for the chip manufacturer: DNA Marking
The cure for the industry: DNA Authentication
In a comprehensive DNA authentication system for chips and semiconductors, embedding DNA marks at the production level is fundamental. A built in certificate of conformance is embedded in each chip that emerges from an OCM. This "certificate" is much more visible, inviolate, and fully portable than any policy or standard.

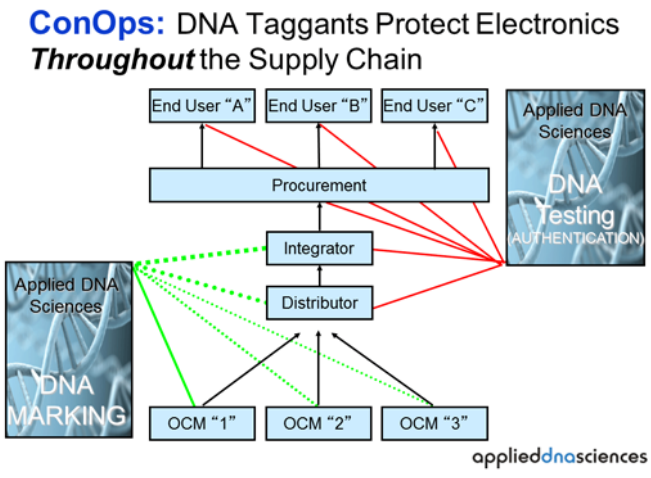
However, the strength of the system is found in the active authentication program by entities downstream: distributors, integrators, board makers, end users. Without active authentication—by which we mean the interdiction of counterfeits at accessible and critical points along the supply chain, and prosecuting the offenders whenever possible—the system becomes dormant, no more than a label claim.
But if the industry and its end users are serious about restricting counterfeits, severely mitigating counterfeit risk, and ultimately marginalizing counterfeit chip purveyors, then these companies will take action by implementing and enforcing the authentication program. The alternative is in the short term to cede an enormous segment of the chip market[6] to a competitor in the form of a loose but malicious network of counterfeiters, and accepting the certainty, sooner or later, of suffering catastrophic reputational damage or worse caused by a critical failure such as in a weapons system or aircraft.

Let us trace the flow of the DNA authentication process. As shown in Figure 4, the procurement entities within the electronics industry typically service a range of downstream end users and engage Applied DNA Sciences in the DNA marking process. Applied DNA works with all of the procurers' trusted supply chain participants, beginning with OCMs who are responsible for marking the chips.

At the distributor, board maker, integrator, or procurement level, authentication nodes are established at accessible and key points, determined by a given supply chain configuration. Statistical confidence levels are established to determine authentication parameters. Lab analysis is then performed, typically in a non-destructive manner, at these nodes.

DNA lab analysis does distinguish absolutely between genuine and counterfeit components. When it does, an unequivocal forensic judgment is declared. The result is a verified flow of authentic components to downstream end users' with counterfeit components fully segregated. This segregation is supported with forensic proof should legal action be deemed appropriate.

Figure 4



If comprehensive, such an authentication network should become highly effective in a surprisingly compressed period of time.

For further information on this technology, please review the Electronics page in the Applications menu on www.adnas.com or feel free to contact one of the authors at media@adnas.com.

References

1 Impacts of counterfeiting and piracy to reach US$1.7 trillion by 2015", February 2, 2011, International Chamber of Commerce

[2] The New York Times, May 1, 2006 "
"Next Step for Counterfeiters: Faking the Whole Company"

[3] Department of Commerce "Defense Industrial Base Assessment: Counterfeit Electronics" (2010)

[4] Lancashire Constabulary, "Problem Oriented Policing Application," June, 2011, p. 8 (unpublished)

[5] "Applied DNA Sciences Successfully Marks Mission-Critical Microchips for the Department of Defense", Press Release, June 22, 2011

[6] According to the National Electronics Distributors Association the IT industry alone **lost $100 billion to counterfeit components** in the year 2010, the last year for which statistics are available. Extrapolating to the economy as a whole including the public sector would certainly result in astronomical figures. Smarter Technology, August 4, 2011