FINAL REPORT

Ultra-secure RF Tags for Safeguards and Security - SBIR Phase II Final Report

Jan. 27, 2015

This report documents the progress for the following DOE SBIR Phase II project over the entire Phase II award period.

Topic: 52. Global Nuclear Safeguards Research and Development

Subtopic: 52a. Safeguards Measurement Sensors

Grant Award No: DE-SC0006260

Project Title: Ultra-secure RF Tags for Safeguards and Security

PI: Dr. Richard E. Twogood
CEO, Dirac Solutions Inc.

Grant Awardee: Dirac Solutions Inc. (DSI)
5776 Stoneridge Mall Road, Suite 255
Pleasanton, CA 94588

Period covered for this report (entire grant period): August 8, 2012 – Dec. 31, 2014

Report Number: DOE-Dirac-06260-1

I. Executive Summary

This is the Final Report for the DOE Phase II SBIR project "Ultra-secure RF Tags for Safeguards and Security." The topics covered herein include technical progress made, progress against the planned milestones and deliverables, project outcomes (results, collaborations, intellectual property, etc.), and a discussion on future expectations of deployment and impacts of the results of this work. In brief, all planned work for the project was successfully completed, on or ahead of schedule and on budget. The major accomplishment was the successful development of a very advanced **passive** ultra-secure RFID tag system with combined security features unmatched by any commercially available ones. These tags have high-level dynamic encrypted authentication, a novel tamper-proofing mechanism, system software including graphical user interfaces and networking, and integration with a fiber-optic seal mechanism. This is all accomplished passively (with no battery) by incorporating sophisticated hardware in the tag which harvests the energy from the RFID readers that are interrogating the tag. Based on initial feedback (and deployments) at DOE's Lawrence Livermore National Laboratory (LLNL), it is anticipated these tags and their offspring will meet DOE and international community needs for highly secure RFID systems.

Beyond the accomplishment of those original objectives for the ultra-secure RF tags, major new spin-off thrusts from the original work were identified and successfully pursued with the cognizance of the DOE sponsor office. In particular, new classes of less sophisticated RFID tags were developed whose lineage derives from the core R&D thrusts of this SBIR. These RF "tag variants" have some, but not necessarily all, of the advanced characteristics described above and can therefore be less expensive and meet far wider markets. With customer pull from the DOE and its national laboratories, new RFID tags and systems (including custom readers and software) for government needs in asset management and tracking were developed. These were tested at a national laboratory and other government facilities, and resulted in immediate procurement actions by the government and deployment of these new systems. Thus, commercialization of the results of this Phase II DOE SBIR was already underway before the end of the SBIR itself. More importantly, operations involving asset management at selected DoE and government sites are already being impacted favorably and could have much broader impacts in the near future.

II. Phase II Accomplishments

Background

Radio frequency identification (RFID) is potentially a key enabling technology for improving the nuclear safeguards monitoring process. A well-designed system could provide invaluable enhancements to the current monitoring practices including: reliable real-time and on-demand monitoring for continuity of knowledge, and improved inspection efficiency without human introduced errors. The RFID system specifications designed for such scenarios will be quite different from commercially available RFID systems such as the ones that are intended to be used in local supermarkets.

In commercial applications, the user is not concerned with a sophisticated adversary, so security is not a primary goal. The users are much more concerned with the cost of the system than with any potential vulnerability that might exist. Hence, the commercial systems being used are adequate for their needs. For safeguards, however, the adversary is highly sophisticated, has extensive resources available, and may have a high motivation to defeat the system. Therefore, serious security measures have to be considered to counter various RFID threats and attacks. The following sections review various usage scenarios for RFID in safeguards applications and describe the requirements of an RFID system designed for safeguards applications.

"Safeguards RFIDs" need to satisfy a number of unique challenging requirements, including:
(1) Reliable tag-reader communications on and around metallic objects,
(2) Low maintenance tags; passive tags that operate without batteries,
(3) Tamper-proof tags that self-destruct upon tampering,
(4) Strong encryption capability to prevent spoofing, relay, and replay attacks,
(5) Strong authentication protocols to secure the identity of tags to prevent monitoring the counterfeit tag instead of the asset.
(6) Packaging for harsh environmental conditions.

The Phase II SBIR project focused on developing a commercial prototype of a tamper resistant, ultra-secure passive RFID tags designed for on metal operations. Major Phase II accomplishments consisted of 1) successful implementation of AES-level encrypted authentication into our passive RFID tags, 2) incorporating a new tag-on-metal structure of our own design, 3) successful tamper-proofing of the passive tags, 4) development of system software including customized graphical user interfaces and networking of multiple readers and 5) development of some potentially important new RFID tag variants which typically have fewer security features but enable new applications that can be met cost-effectively.

Project Tasks and Progress

Table 1 below shows the tasks proposed for the entire 2-year Phase II project (the schedule for these tasks is addressed in the next section). Table 2 below shows the original proposed schedule. It should be noted that the Phase II project was given a no-cost time extension extending the end-date from August 7, 2014 until December 31, 2014. Since the vast majority of work was conducted with the schedule of Table 2 as proposed, we have included it for reference.

Tasks	Objectives	Milestones
Task 1. AES Authentication	To add optimized AES encryption on passive tags with high read rate.	Milestone 1.1: Tag Authentication and Customization Milestone 1.2: Optimizing the Speed of Tag Read Rate
Task 2. Tamper-Proofing and Mounting of Tags onto Metal Cylinders	Mechanical design and innovations for disabling the tag electronics upon removal	Milestone 2.1: Design and implementation of tamper proof tags
Task 3. Tag Packaging for Field Deployment	To provide various type of electronics packaging for various safeguards scenarios including field hardening for autoclave and radiation environments.	Milestone 3.1: Tag packaging for few units Milestone 3.2: Testing and performance verification Milestone 3.3: Packaging large number of tags
Task 4. Graphical User Interface	Customized user friendly interface to report detection state of RF tags and validation of authenticity.	Milestone 4.1: GUI software development
Task 5. Network of readers	To cover a large area with continuous monitoring	Milestone 5.1: Customized reader networking protocol Milestone 2: Reader installation and infrastructure design
Task 6. Database Management Software	To translate the received data from multiple readers to user-friendly messages regarding the tagged item's presence and absence or its location.	Milestone 6.1: Database software development for managing data into a central data repository
Task 7. iPhone reader with AES	To have easy access to reader data on an iPhone	Milestone 7.1: iPhone application development
Task 8. Small-scale manufacturing	Flexibility in design changes to address multiple customers	Milestone 8.1: Low volume manufacturing of tags
Task 9. Initiate ASIC design of tags	To carefully plan for all steps of mass production with first pass success to avoid possible re-designs	Deliverable 9.1: Report on ASIC planning

Table 1: Summary of Tasks

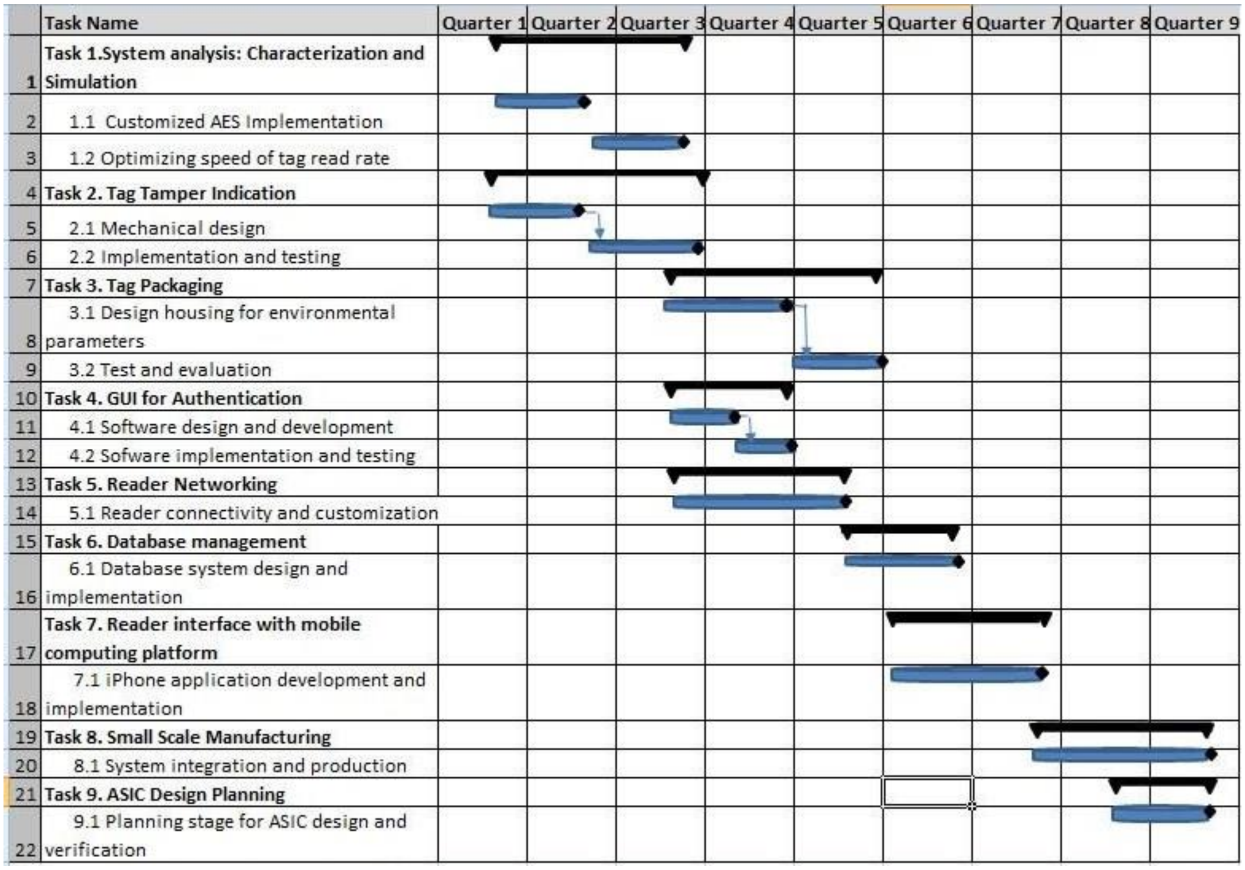

Table 2. Schedule for Phase II SBIR project

We now briefly describe these results on those tasks.

Task 1 results – DSI has implemented a full AES implementation onto the commercial prototype tag, hereafter referred to as the LLNL-DSI passive RF tag. The LLNL-DSI passive RF tag currently operates in the unlicensed UHF band with operational frequency of 915 MHz. The tag is designed to have flexibility and adaptability to other operational frequencies in UHF band accepted by other countries (i.e. European UHF band is 862 MHz). This tag is designed for operations on metallic environments using unique and innovative tag antenna design. Without any on-board batteries, the LLNL-DSI tag is capable of collecting enough power from its reader antenna from a long range to send data by only "reflection and backscatter technology" (no active transmission).

DSI has developed and implemented strong encryption (AES) and dynamic data authentication capability into this passive tag. The strong AES encryption ensures that the data cannot be translated or decoded by an adversary while dynamic data authentication prevents the cloning as well as recording and replaying the tag message by an adversary. In the dynamic authentication function, the reader sends random messages every 1 second that are only recognized by the tag (shown in Figure 1). Therefore, the tag cannot be replaced by any commercial tag since it cannot respond to the authenticated code every second.

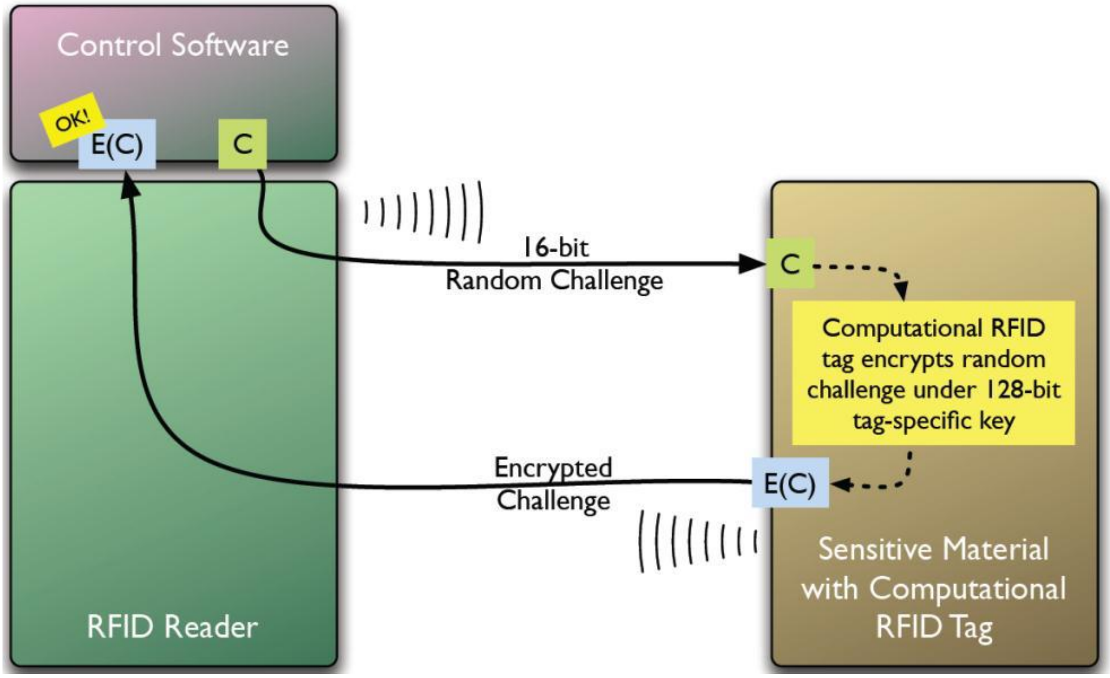

Figure 1: DSI's dynamic authentication AES algorithm used on LLNL-DSI passive tags.

In the current form this tag can be read from a distance of 200 ft without encryption and authentication; with encryption and authentication capability the tag-reader communications is 15 ft (required by IAEA). It is important to emphasize that there is no battery on this system and it operates totally passively with indefinite lifetime.

Task 2 results – Dirac Solutions and Lawrence Livermore National Lab (LLNL) collaborated to develop an initial tamper-proof capability on the LLNL-DSI tags. In addition to the concept development, DSI is pursuing joint patenting of this work, and looking into manufacturing at DSI and its contractors for an initial scale-up if needed. With respect to physical security, the tag has a unique design where the RFID chip is destroyed mechanically upon any removal attempt. This unique design is literally a "miniature guillotine" waiting to irreversibly destroy the RFID chip and its memory once the tag is attempted to be removed. Figure 2 shows the trigger pin in the back of the passive tag.

Figure 2: Bottom view of the secure passive tag shows the trigger pin to activate the miniature guillotine for self-destruction mode.

Task 3 results (tag packaging) – This task addresses various types of electronics packaging for safeguards scenarios including field hardening for possible autoclave and radiation environments. DSI and LLNL have already completed an initial packaging of the tags and they were tested successfully as early as December 2012 in NA-22 tests in Nevada. A preliminary analysis of the issues regarding possible autoclave conditions has been undertaken. Initial results of the analysis lead us to be optimistic that the autoclave conditions are achievable, but will likely need modifications of the materials used in the R&D prototype LLNL-DSI passive tags. In addition, there seems to be somewhat ambiguous information as to whether a requirement of nuclear autoclave conditions is absolutely essential. It may be that it is in some scenarios (e.g. the original primary application target, tagging of UF6 canisters for the IAEA) while there may be many other cases where that is not needed.

Task 4 results (GUI software) – While the original schedule called for the Graphical User Interface (GUI) software for the tags and readers to begin in early 2013, LLNL requested whether DSI could accelerate that effort as well, due to the a DOE field testing for another project. DSI concurred, and rapidly developed a GUI that was successfully deployed by LLNL at the tests. Figure 3 shows a sample output of the interface. This GUI software has been readily modified to address specific customer needs for the deployments of the ultra-secure tags and the less-sophisticated passive tags described later in this report.

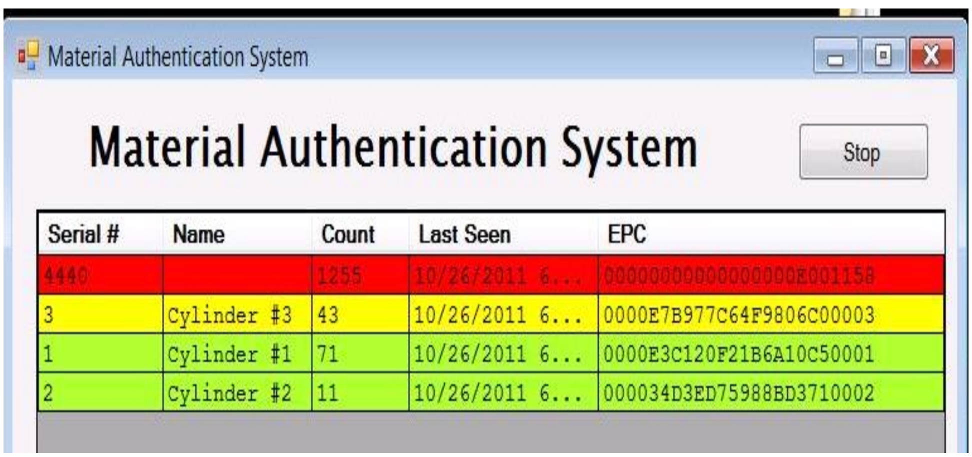

Figure 3: Graphical User Interface for passive tag system

Task 5 results (networked readers) – DSI developed an initial networked reader capability during early 2013, ahead of schedule. That earlier-than-planned effort was also driven by a request by our national lab partner (LLNL) to provide at least rudimentary networking for their NNSA-funded program using these passive tags. Furthermore (and beyond the original task proposed), DSI developed the networking of tag readers to cover a large area for monitoring. The capability also allows space zone definition per reader, which in turn allows tracking of tagged items. This is a bonus capability of the system that might prove quite effective in item tracking.

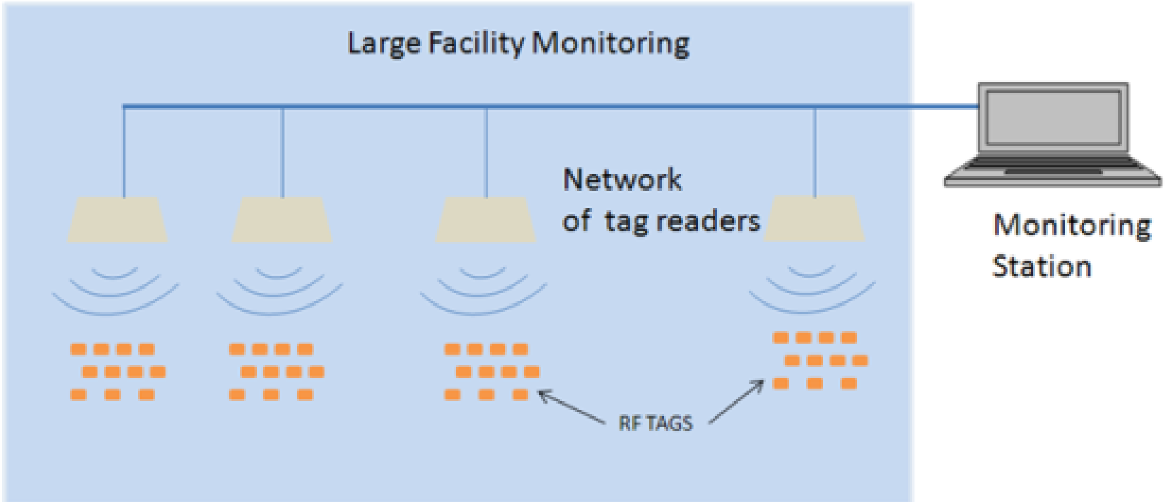

Figure 4: Network of RFID readers for real-time monitoring of large facilities developed in Phase II.

Task 6 results – Database Management Software

The database management for RFID tags, particularly for government applications, is often highly dependent on the applications and facilities targeted for deployment. While LLNL was testing and deploying our ultra-secure tags and other DSI "variant tags" derived therefrom, an application need was identified by LLNL at DOE's JTOT facility in New Mexico. This application used hundreds of DSI tags for inventory management and required database software development for managing data into a central data repository at that facility.

DSI successfully developed the software to port the DSI RF tag data from the DSI/LLNL readers into the central database. That software is now the baseline code for the planned deployment of DSI tags and readers into several DOE facilities in 2015. Care has been taken to ensure most or all of the code base can be used for future deployments of not only the tag variants being deployed now, but also the ultimate deployments of the ultra-secure RF tags likely to begin in late 2015 or early 2016. Figure 5 shows the GUI associated with DSI's real-time inventory and database management deployed to JTOT facility.

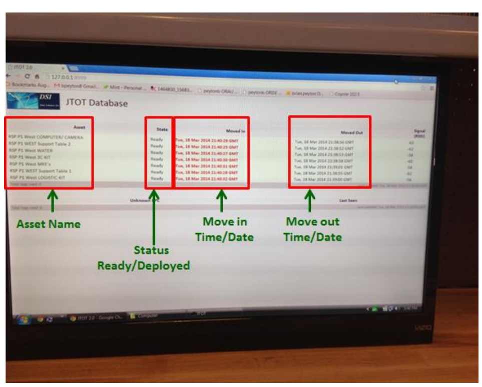

Figure 5: Real-time inventory and database management developed in Phase II.

Task 7 results – iPhone reader with AES

This task was conceived with the goal of developing an “iPhone-like” handheld reader capability for the ultra-secure RF tags. Early in the project DSI determined there were numerous possible handheld reader options that might make sense in terms of functionality, including tablets and small existing handheld readers developed by commercial RF companies. With no clear concept-of-operations for the ultimate use of the ultra-secure tags (and none likely for at least a year or two), DSI worked with LLNL to determine what would be most useful for the short-term DOE needs for test/deployment of the tags.

In addition to the programmatic testing by LLNL of the ultra-secure tag, other DOE applications for the broader set of “tag variants” (see Section III below) were becoming evident. LLNL determined it would need a variety of readers, from briefcase-sized UHF systems for fielded systems to small handheld readers. A briefcase-sized reader with full software functionality (including dynamic encrypted authentication) was jointly developed, and DSI designed and built a version for commercial production called the DSI PR110. For the handheld functionality, two thrusts have been pursued.

1) Semi-custom handheld reader: DSI has procured an existing Motorola UHF handheld reader and has modified the software to provide encrypted authentication for DSI’s ultra-secure tags with an interface to iPhone and iPad (Android interface is possible also). Another version of this reader with database capability (without encrypted authentication) is scheduled to be deployed to NNSA Nuclear Emergency Responders at PANTEX (JTOT, RAP4, ARG) as well as NRGROC.

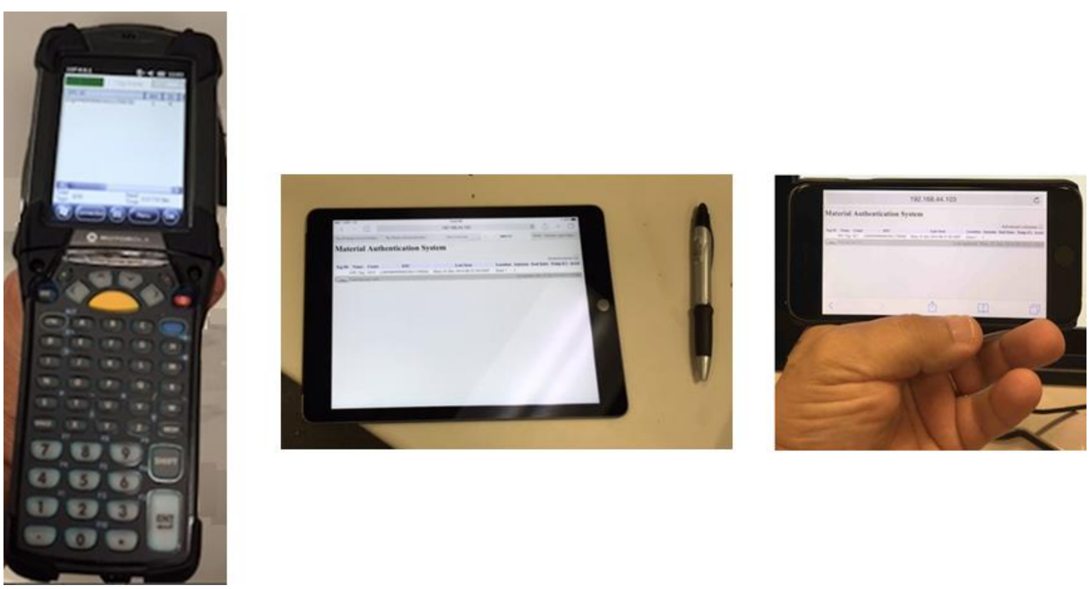

Figure 6: DSI’s semi-customized handheld reader with iPad and iPhone interface

2) <u>Fully customized handheld reader:</u> LLNL and DSI have collaborated on design of a fully customized handheld reader. This effort consists of both hardware and software development as well as antenna design and integration. An early functional prototype of this system is available as of the end of the Phase II SBIR. However, more laboratory and field testing and evaluations are needed before the packaging process starts.

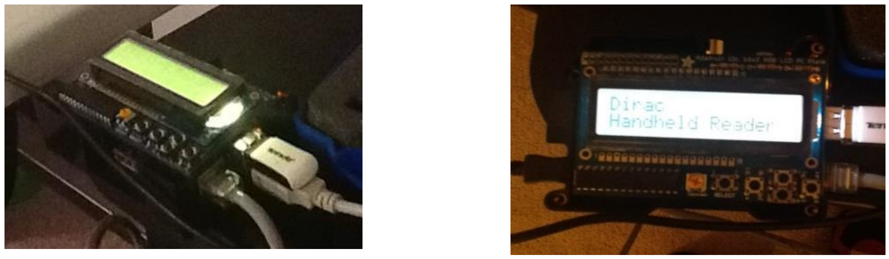

Figure 7: Components of DSI's fully customized handheld reader

Task 8 results – Small-scale manufacturing

Following the success of developing the capabilities described above (dynamic encrypted authentication, tamper-proof mechanical device, and supporting software systems), hardware sufficient to build a set of 10 tag systems was developed. Five of those tags have been fully integrated and tested successfully; components for the other 5 are in hand at varying degrees of readiness. Several of these tags were provided by DSI to LLNL to use in the DOE-funded test deployments described earlier.

An initial investigation into the cost points that can be reached for production of hundreds, thousands, and tens of thousands of these ultra-secure tags was conducted, with or without further enhancements such as ASIC integration of some of the electronics. The results were promising, indicating the pricing per tag can clearly be driven down to the few hundreds of dollars per tag level – a price point stated to be acceptable by several potential end-users.

Task 9 results – Initiate ASIC design

Based on the successful prototype tag development, test and deployment by a national lab, we began a detailed study of options for proceeding to ASIC integration of some or all of the electronics in the tag. This included discussions with LLNL personnel familiar with this project and with ASIC design experience; an ASIC company; and university personnel actively involved in the electronics and energy-harvesting used in our ultra-secure tags.

A preliminary path forward into Phase III was identified with a university partner, details of which have been provided to the Department of Energy in the Phase III proposal process and contracting discussions. ASIC integration of some or all of the electronics has been scoped out and parsed into 3 different phases. The first phase involves low risk and results in ASIC integration of the energy harvesting electronics and associated interfaces. The second phase, with moderate risk, involves ASIC integration of some of the functionality in the processing functions the RF tag performs, but maintains a separate microcontroller for the more complex functions. This second phase, which most likely can be accomplished within the existing proposed Phase III effort, will result in an ASIC chip interfaced to another existing chip, with improved RF tag performance. The third phase, which is high risk and will likely require identification of additional funding beyond that already contemplated, would involve complete integration of all functionality into one chip. That third phase would likely involve the licensing from a major company of the chip design files of an existing microprocessor.

<u>Bonus deliverables</u>

There have been several important developments that have extended the opportunities for this SBIR Phase II to have broader impact, and achieve early commercialization successes, earlier than projected at the beginning of phase II. Our success in demonstrating and low-volume manufacturing of specialized "ultra-secure" passive RF tags in phase II allowed us to identify new possibilities that went well beyond safeguards applications. To address these new markets, as a bonus deliverable, we developed potentially important new RFID tag variants – ones which went beyond the original planned scope but whose lineage derives from the core R&D thrusts of this SBIR.

These new tag variants that emerged during Phase II include 1) active tag implementations that leverage the encrypted-authentication techniques developed in this SBIR, 2) active tags with sensor inputs, with or without the AES-level authentication, and 3) simpler passive tags with tag-on-metal capability borne from the Phase II passive tag work, but with fewer security features. Figure 8 shows new tag variants derived from the original passive "ultra-secure" tags.

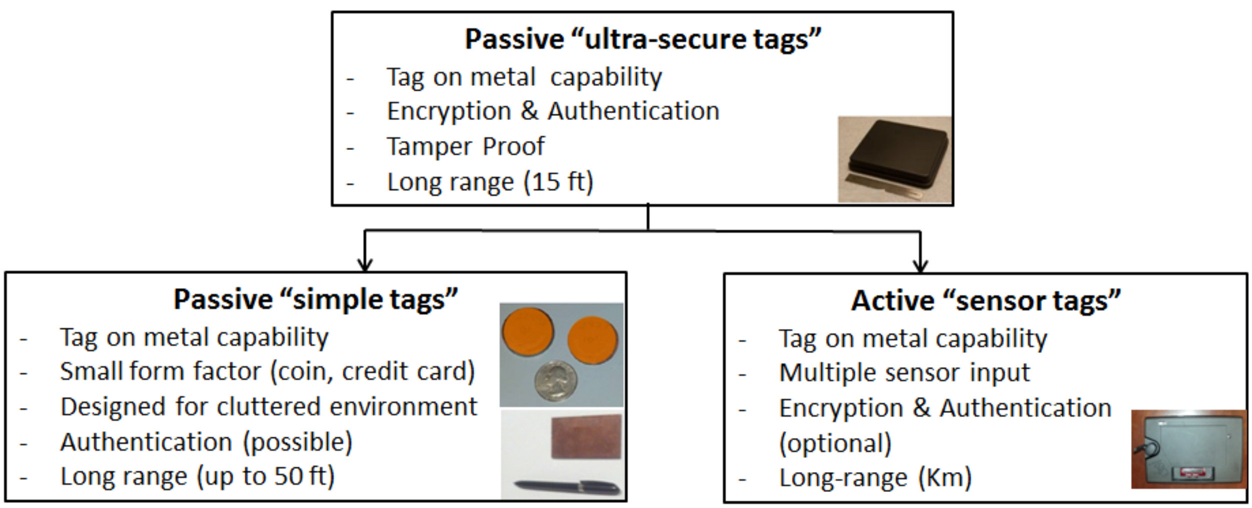

Figure 8: DSI tag portfolio developed in Phase II

Following is a bit more detail on these tag variants that have emerged from the core Phase II effort focused on ultra-secure tags.

Active tags - At the outset of this Phase II activity, DSI was asked by LLNL to explore whether the AES encrypted authentication technology in the LLNL-DSI passive tags (the focus of this SBIR) could also be utilized in active tags that are battery powered. The reason was that for the upcoming field test for the Chain of Custody program, there was a need for tracking objects at greater ranges, and active tags allow longer ranges. DSI put high priority on this and designed and developed an active tag which had the AES authentication needed, but not the other aspects of the LLNL-DSI passive tag such as tamper-proofing and energy scavenging. This tag, which is now called the DSI AT200, was also fielded successfully at the same Nevada test. Figure 9 shows the AT200 tag.

Following that, another ARPA-E program funded at LLNL requested a version of the DSI AT200 active tag, but with the following changes: a) no encrypted authentication requirement, and b) sensor inputs into the tag for relay from tag to reader. DSI modified the AT200 (hardware and software) to accommodate that need. The resulting "tag" is now called the AT100 and DSI is considering possible extensions of that capability.

Figure 9: Active tags with sensor input and optional data security (AT200)

After Phase II, we plan to miniaturize these active tags to the size of a credit card and make them available for applications that require long-range sensor data transmission at long battery life of minimum 5 years. These tags will share the same circuit boards as secure passive tags, so optimizing the circuit boards and preparation for ASIC design will benefit both active and passive tags, complementary capabilities that can serve a variety of markets.

Simple passive tags on metal – One of the Phase II bonus deliverables was the development of new high gain simple passive tags with long read range and optional authentication capability. A variety of these tags were developed as prototypes with their dimensions ranging from a coin size to credit card size and larger at 4"x7". These tags with new antenna design are targeted towards highly cluttered environments were large amount on obstructions exist between the tag and the reader antenna. Figure 10 shows the portfolio of such simple tag prototypes.

Figure 10: Family of DSI's simple tag prototype for various applications.

This set of RFID tags have an immediate customer and a subset of those are being deployed to Joint Technical Operations Team (JTOT) for real-time inventory management of their equipment needed for nuclear emergency response operations. The first system being deployed in March 2014 includes:

several hundred of the PT210 2"x3.5" credit-card sized "parent tags" shown in Figure 11a, a custom RFID reader with custom antennas, and DSI database management software.

(a) 2" x 3.5" PT210 passive tag

(b) 4" x 7" PT110 long-range passive tag

Figure 11: Field hardened passive tags manufactured for deployment to JTOT operations.

These tags are being built to be used for automated portal monitoring of pelican cases (called "The Parents" in JTOT database) full of equipment needed for nuclear emergency response operations. Even smaller size (1" x 1.75") tags (not shown) will be used in the next deployment in 2015 for monitoring equipment inside the pelican cases (called "The Children" in JTOT database). The RFID reader data is being integrated with JTOT's current database to enable JTOT operators to analyze information at various abstraction levels such as items unique ID, time, location, and other information about their deployment.

These "bonus" deliverables were briefed to the program office for this SBIR in 2013 and 2014. It was generally agreed that these extensions of this SBIR Phase II project should continue to be pursued and considered additional payoffs of this SBIR. This makes sense in light of the direct technical lineage enabled by this SBIR. However, DSI has used internal non-SBIR funds for any such efforts once they reach the point of buying hardware or manufacturing multiple tags for any other agency other than DOE NA-22.

In summary, all originally scheduled project goals and milestones were met for the SBIR project, with a few minor variations based on input from the DOE national labs. Furthermore, the original project goals were far exceeded in that additional unplanned technical spin-offs and applications have emerged and resulted in government acquisitions and deployments.

Ultra-secure passive tag integration with fiber optics seal – Another phase II bonus deliverable was to collaborate with LLNL for low volume manufacturing of a new generation of ultra-secure passive tags that are integrated with fiber optics seals. These unique tag-seal units are targeted towards safeguards markets where the seal status is continuously monitored and reported through secure encrypted authentication without the need for any batteries. Figure 12 shows the Ultra-secure passive tag-seal unit.

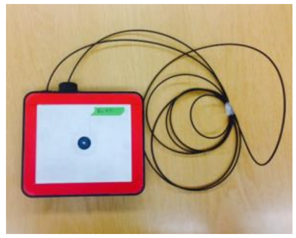

Figure 12: Passive tag-seal for safeguards applications, manufactured in Phase II.

III. Project Products, Intellectual Property, and Other Outputs

The following are some of the intellectual property, publication, tech transfer, collaborations, and other products developed that are worth mentioning:

1) Key Product – The prototype DSI-LLNL tags shown in Figure 2 (the main product of this SBIR) were completed and tested successfully by LLNL in Nevada. DSI owns the key intellectual property in the tag, including all software rights and the tag design itself. DSI is considering the options of patenting the tag design; at the time of this report it remains DSI trade secret information. DSI will own jointly (with LLNL) the tamper-proof concept. This ultra-secure passive RFID tag is likely the most sophisticated and secure RFID tag in existence.

2) Other Products – As mentioned above, an entirely new active tag (DSI AT200) has been developed. DSI is proceeding with the belief that it benefits both DOE and DSI to have some linkage to this SBIR as it will lead to additional "return on investment" from this work for both parties to claim.

Based on the AT-200 active tag, DSI has developed a similar tag without AES authentication but with sensor inputs for new applications requiring sensor/tag integration. This product is called the AT-100.

Furthermore (and as described above), another family of simple passive tag based on the technologies pioneered in this SBIR has been developed. That tag (passive; tag-on-metal capable; no encrypted authentication; no tamper-proofing) has already attracted government sponsor interest from the DOE and initial purchases from the government are being delivered on.

3) Patents– A patent application for the tamper-proofing mechanism in the LLNL-DSI tags has been prepared and submitted to the USPTO. This patent will be jointly held by DSI and LLNL. As a result, DSI holds commercial rights to the new tamper-proofing mechanism.

A provisional patent, also joint between LLNL and DSI, has been filed for a secure optionally passive RFID tag with external power source and data logging.

4) Collaboration – As described briefly herein, and in more depth in the original Phase II proposal and commercialization plan, there was an extensive joint collaboration between LLNL, DSI, and their contractors in this project. Figure 13 below shows a top-level description of this joint effort. There are many aspects of this collaborative program, only some of which have been mentioned in this report.

In terms of a simple bottom line: DSI's assessment is that this is an extremely successful collaboration. The careful coordination among all parties, strong and supportive DOE management, and the mutual strengths of the teams have multiplicative effects that no single institution could likely achieve. As a result, important results are being achieved and significant, multi-agency and possibly commercial payoffs are highly likely.

5) Possible strategic relationship(s) - DSI has been approached by one company with an interest in providing manufacturing for the passive tags (and now possibly active tags as well) and either licensing or jointly marketing the tags. Similar discussions regarding possible strategic collaborations, licensing discussions, and related activities are underway. Some of these are with representatives of possible collaborators; some are with existing business partners who have indicated interest in being involved in finding strategic partners. Most details are business sensitive or DSI proprietary, but can be shared with DOE program management if requested.

6) Software – The software developed to date includes the encrypted authentication passive tag software (funded by DSI as discussed earlier), the GUI software, networking software, and database management software. Much of the new code development itself was funded by DSI internal resources, and some of the code base is open-source from others. Some of the code was altered under this SBIR project to meet the specific needs of the project and the national laboratory needs for some customization. DSI has taken care to ensure it has all commercial rights to the entire code base and has already made executable versions available for government procurement.

7) Publications – DSI has to date been conservative on "advertising" or publishing the core results of this project. Reasons include preliminary (and pre-patent) technical results, bi-lateral collaboration with a national lab, joint IP development, and DSI's own venture-type strategy of remaining in "stealth mode" at some level on product details until commercial versions are ready. The first publications of Phase II results are in the following: [1] Richard E. Twogood, *"Ultra-secure RF Tags for Safeguards and Safeguards and Security,"* UITI conference, Lansing, MI, June 5, 2013, and [2] Richard E. Twogood, *"Ultra-secure RF Tags for Safeguards and Safeguards and Security,"* UITI conference, Walnut Creek, CA, June 3, 2014.

The big picture – We described above in some detail the Phase II SBIR results to date. To put this all in perspective, Figure 13 shows the basic high-level framework for this entire effort. We have also included the relevant portions of the DOE NA-22 funded effort at LLNL which provide key technology components that this DSI SBIR effort has leveraged.

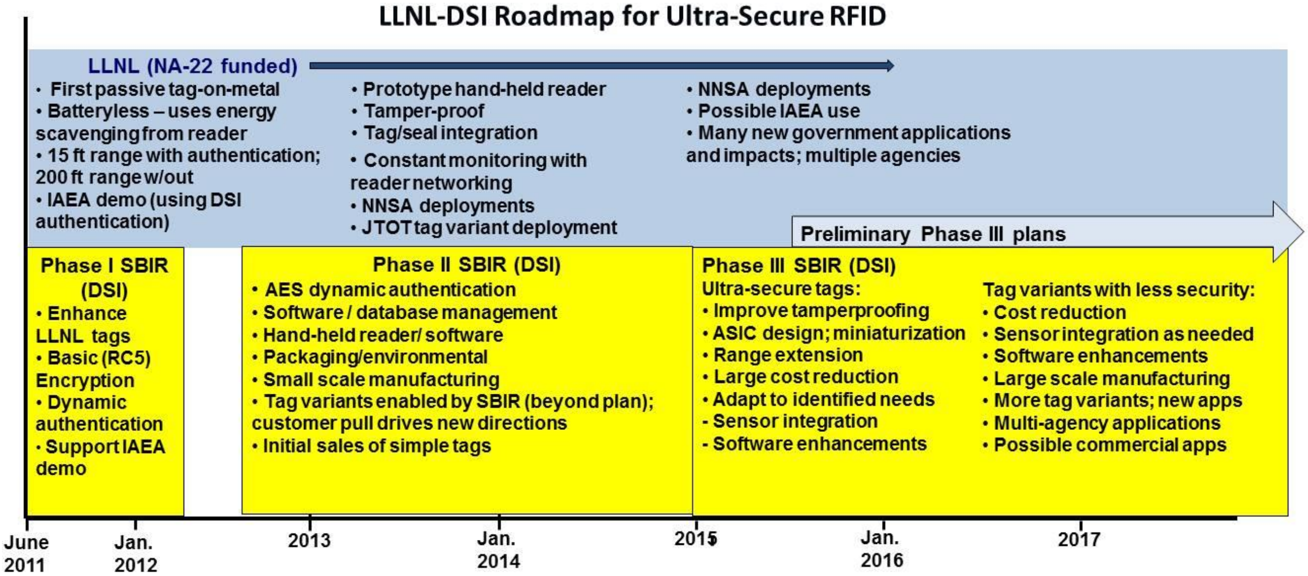

Figure 13: Breakout and timeline of joint efforts between DOE/LLNL and DSI

It is worth mentioning that Figure 13 lays out a tentative path forward following the Phase II project (the subject of this interim progress report). DSI has proposed a Phase III effort to the DOE NNSA and indications are that that work will be funded. That effort will focus on extending the Phase II results, with particular emphasis on ASIC-level integration of some or most of the electronics in the ultra-secure RF tags; possible enhancement of the tamper-proofing mechanism; cost reduction to meet the price points identified by the government and IAEA potential adopters; and initial deployments to those adopters via procurements or other collaborations.

Other Phase III efforts are planned with a primary focus on expanding the deployment and sales of many of the tag variants and systems described above. Moving forward from the early adoption in 2014 of the "parent" tags by the DOE, there are planned 2015 deployments at several government facilities. Preliminary procurements are already underway, including procurement actions being negotiated with 3 government entities as of early 2015. It is those emergent adjacent RFID tag system opportunities, enabled by the Phase II SBIR, which are expected to have the most immediate payoff to government end-users.

On the international front, collaborations are under discussion with several entities. Discussions with the IAEA in Washington DC and Vienna in late 2014 have led to their strong interest in some initial procurement and testing/evaluation of the ultra-secure tags. Meetings and tag demonstrations with ISPRA (in Milan, Italy) and Schlumberger (in Paris, France) have been arranged for the spring of 2015. The nature of any procurements and foreign collaborations will be determined pending decisions by and discussions with DOE NA-22 regarding their role in the post-Phase II SBIR activities.

Return on Investment - It is obviously far too early to predict most of the ultimate outcomes and long-term impacts of this SBIR project. For instance, adoption by the IAEA of the highly-secure passive tags (or variants thereof) depends on factors beyond the control of DSI, or even the DOE. Nonetheless, as of the end of this Phase II SBIR it is clear that this effort will result in at least moderate, and more likely large, impacts. At a minimum, DSI expects 1) multiple government program impacts, almost certainly multi-agency, 2) products generated as expected, as well as new products beyond the original plans, and 3) commercialization success of at least moderate (say 1:1 to 5:1 Return-on-Investment, or ROI) and more likely large (5:1 – 50:1 ROI or more) in less than 10 years. As measured by ROI=(total DSI revenue generated to date from SBIR results)/(SBIR funding), the ROI was already circa 0.5:1 at the end of the Phase II SBIR. From initial commitments (including verbal commitments from government offices) we expect the ROI to exceed 2:1 by the end of 2015 and likely 4:1 by the end of 2016. After that things are less certain, but these initial successes have led to DSI projecting, for its planning purposes, ROI exceeding 10:1 by 2018 and exceeding 30:1 by 2021. By any measure, these are extraordinarily positive results and indicative of both the preliminary and the potential success of this SBIR project.

IV. Summary and Conclusions

This Phase II SBIR project focused on the development of an ultra-secure RF tag with security attributes identified as important by the DOE and IAEA for the securing of valuable assets such as nuclear materials. A prototype tag was successfully designed and multiple tags were built, tested, and deployed in DOE-funded field experiments by a national laboratory. The AES standard encryption has been successfully completed, ported to the initial tag prototypes, and tested successfully by the Lawrence Livermore National Lab team using these results for a DOE program sponsored by the program office responsible for this SBIR. The initial tamper-proofing design has been conceived, implemented, and also successfully tested at the same DOE field tests. The Graphical User Interface software for this next generation passive tag was developed; networking of readers was implemented and tested; and initial database management software was also implemented. Manufacturing at low levels was accomplished, and scaling to larger levels investigated and determined to be manageable.

Furthermore, additional advances have been made on new parallel paths that exploit the results from the ultra-secure RF tag R&D. These include 1) active tag implementations that leverage the encrypted-authentication techniques developed in this SBIR and/or other selected capabilities from the passive tag work; 2) active tags with sensor inputs; and 3) simpler passive tags with tag-on-metal capability but fewer security features. The simpler passive tags (and related RFID readers and software DSI has developed) have already been tested, procured, and deployed by the DOE. Multiple future deployments which will require procurement of these systems from DSI have already begun as of late 2014 and early 2015. As a result, commercialization of the results of this SBIR is already underway and will likely have significant impacts in government, and possibly international and commercial, applications.