Table 1: Quality Gates

Item	Test	Criteria
1	Receiving Inspection of the Sensor and circuit verification	Dimensions
2	Resin	Chemical analysis
3	Visual Insp. of the Sensor prior to folding	Damage & contamination
4	VI Sensor after folding	Proper folding
5	Electrical verification of sensor after folding	Sensor circuits
6	Electrical verification after sensor cure	Current circuits
7	PU Material Properties	Stoichiometry & cure
8	VI after PU dispense	Physical appearance
9	Electrical verification after resin	Sensor circuits
10	VI after Crypto to PCI merge	Solder defects
11	PCI compliance	Thickness gage
12	Burn-in	Functional Test

SUMMARY

The combination of a sensor mesh and monitoring circuitry provides an environment that protects sensitive data from cyber theft. It is manufactureable and reliable both in preventing undesired access and its longevity in the field.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the following contributors: Assistance provided by Vincenzo Condorelli, Nihad Hadzic, and William Santiago Fernandez of IBM Poughkeepsie, NY toward the content of this paper. We would also like to acknowledge the team who have worked on this project: Dave Allan, Ed White, Frank Orapello, Jason Wertz, Jim Wilcox, Jing Zhang, Mitch Ferrill, Nandu Ranadive, Norm Curry, Stu Lake and Tim Donahue.

REFERENCES

1. Gore is a trademark of the W. L. Gore & Associates, Inc. Newark, DE.

2. T. W. Arnold, C. Buscaglia, F. Chan, V. Conderelli, J. Dayka, W. Santiago-Fernandez, N. Hadzic, M. D. Hocker, M. Jordan, T. E. Morris, Jr. and K. Werner, " IBM 4765 Cryptographic Co-Processor," IBM Journal of Research and Development, Vol. 56 No. ½, pp. 10:1-10:13.

3. Arnold, T., Dames, A., Hocker, M. D., Marik, N., Pellicciotti, A. and Werner, K., "Cryptographic system enhancements for the IBM System z9", IBM Journal of research and Development, Volume 51 Number 1.2. web site: http://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=5388699&punumber=5288520

4. Woodard, S. E.., Functional Electrical Sensors as Single Component Electrically Open Circuits Having No Electrical Connections, IEEE Transactions on Instrumentation and Measurement, Vol. 59. No. 12, December 2010, pp. 3206-3213.

5. Eren, H. and Sandor, Lucas D., "Fringe-Effect Capacitive Proximity Sensors for Tamper Proof Enclosures," Proceedings of Sensors for Industry Conference, Feb. 8, 2005, pp. 22-26.

6. Liebholz, Stephen W., "Solutions for the grand Challenges of Information Security: Protection Against Rogue Insiders, Dynamic Compartmentalization and True Quantum Encryption." Proceedings from 2007 IEEE Conference on Technologies for Homeland Security, pp. 129-132.

7. Paul, P., Moore, S. and Tam, S., "Tamper Protection for Security Devices." from the proceedings of the 2008 Symposium on Bio-inspired Learning and Intelligent Systems for Security, pp. 92-96.

8. Isaacs, P., Buscaglia, C., Feger, C., Pearsall, K., Wolf, H., Cesana, M., Moscheni, G., Cuthbert, K. and Hunter, S., "Packaging and Processing of a State-of-the-Art Encryption Technology." From proceedings of 2007 IMAPS Symposium, San Jose.

9. National Institute of Standards and Technology Cryptographic Module Validation Program (CMVP). website: http:/csrc.nist.gov/groups/STM/cmvp/index/html.

10. IBM 4765 PCIe Cryptographic Coprocessor Installation Manual. web site: http://www-03.ibm.com/security/cryptogards/pciecc/pdf/4765install.pdf.

11. Tamper Respondent Mesh is a trademark of the W. L. Gore &Associates, Inc. Newark, DE.

12 Gore Anti-Tamper Physical Security for Electronic Hardware. web site: http://www.gore.com/en_xx/products/electronic/anti-tamper/anti-tamper-respondent.html.

13. Maxim Integrated DeepCover™ Security Manager (DS3645). web site: http://www.maximintegrated.com/datasheet/index.mvp/id/5424.

14. IBM Engineering Specification, PCIe Cryptographic Coprocessor Secure Module Assembly Requirements, written by IBM and SEM, Services for Electronic Manufacturing, Milano, Italy.