

# Hardware Intrinsic Security: Fables Perception and Awareness

Chelsea Boone<sup>1</sup> Pim Tuyls<sup>2</sup>

<sup>1</sup>Global Semiconductor Alliance

<sup>2</sup>Hardware Intrinsic Security Initiative

Counterfeiting, which includes both cloning and overproduction, is a serious and growing concern for the electronics industry. KPMG and the Alliance for Gray Market and Counterfeit Abatement (AGMA) have estimated that 10 percent of high-tech products sold globally are counterfeit. The availability of technology to counterfeiters is helping increase the threat. With sophisticated tools such as focused ion beams and scanning electron microscopes at their disposal, today's counterfeiters are able to breach many traditional key-storage systems, costing semiconductor and systems companies billions of dollars in lost revenues. A key leading indicator of counterfeiting issues is the increase in product discounts. With the increase in online sales, companies need to monitor this channel for counterfeiters as well. A report published by New Momentum revealed that actual revenue lost when tracked through online sales was higher than predicted.

Today most semiconductor companies outsource some or all of their manufacturing, yet many have not put in place monitoring systems to identify and keep out counterfeiters. For example, a large electronics

company that outsources its manufacturing needs to protect its products from overbuilding during the manufacturing flow and from cloning once they are in the field. Hardware security systems use secret keys to verify the authenticity of products. When challenged, an authentic product will use that secret key to prove its authenticity. Clearly, the security of this key is paramount: Counterfeiters who gain access to the secret key can have their products incorrectly register themselves as authentic ones. With the introduction of a new approach known as hardware intrinsic security (HIS), GSA and the HIS Initiative collaborated in mid 2010 to determine perception and awareness of counterfeiting, secret key storage and the new HIS approach by fabless companies. The collaboration resulted in an online survey and report. This article contains the key findings from this study.

## **Strong Interest in Secret Key Storage Driven by End Markets and Unique Identification**

One of the most significant findings is that 47 percent of survey participants said they need secret key storage in 2011. Forty-eight percent of participants indicated

secret key storage is currently a feature or requirement from their customers. An additional 40 percent indicated that the need for secret key storage is dependent on their customer. This is consistent with the hypothesis that some markets are more likely to adopt HIS solutions because of their higher margins, making them more

of a target for counterfeiters. The survey participants' primary markets and the market applications selected for implementation of secret key storage were similar, which is not surprising since the survey was voluntary. Networking and telecom was the top-ranked market application among participants, with 17 percent select-

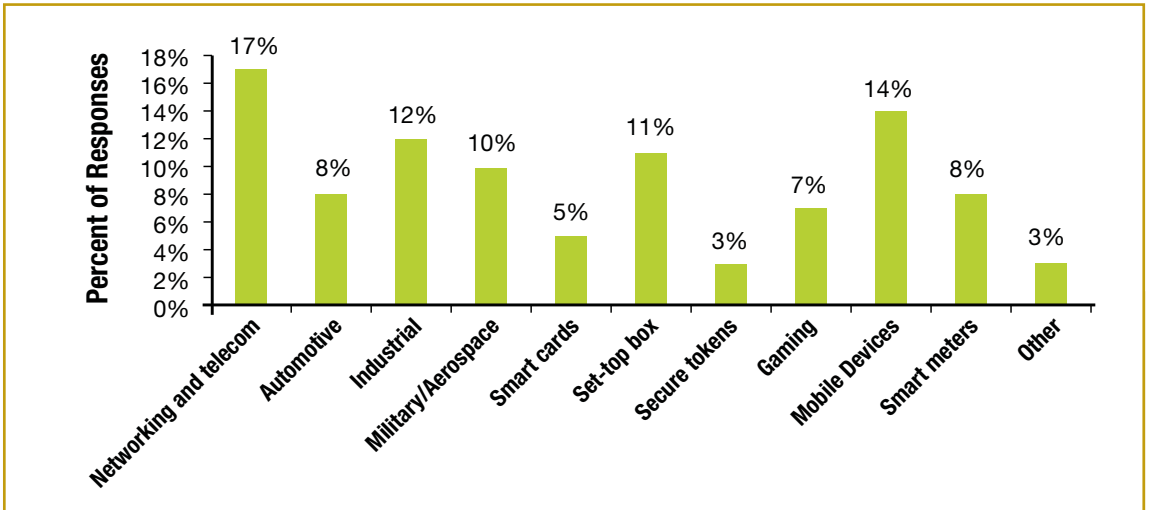


Figure 1. Networking and telecom was the highest-ranking market application for implementation of secret key storage in 2011.

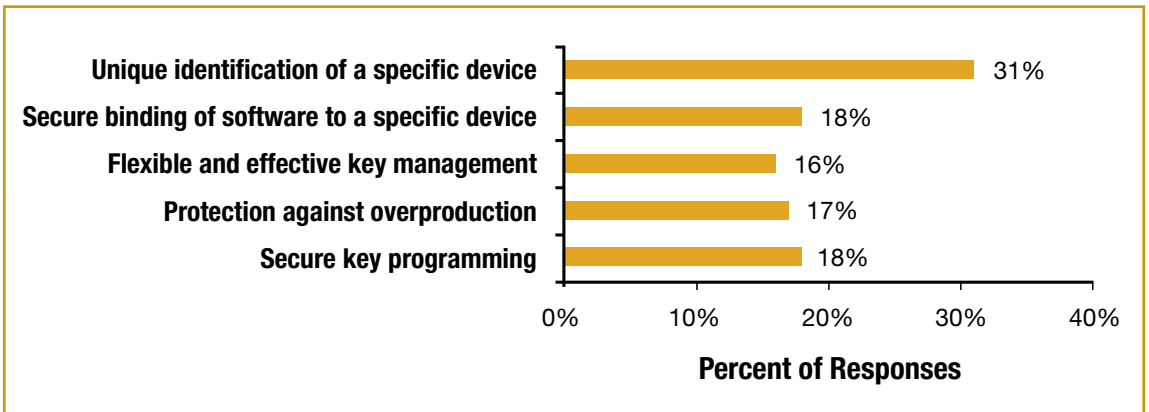


Figure 2. Unique identification of a specific device is the dominant reason given by survey participants for adopting secret key storage.

ing it. This is consistent with the view that participants that target product segments with higher margins will be more interested in secret key storage due to the higher risk of counterfeiting. Mobile devices came in second, at 14 percent, and was followed closely by industrial, set-top box and military/aerospace (Figure 1).

Unique identification of a specific device ranked as the top driver for secret key storage adoption, with 31 percent of responses. Secure binding of software to a specific device and secure key programming were tied for second, with 18 percent of responses (Figure 2). This result was slightly surprising to a few HIS Initiative advisers who had anticipated secure binding of software to a specific device to be the No. 1 response. This result possibly reflects the high degree of outsourcing by GSA members and that most participants were semiconductor companies and not systems companies.

## Awareness of Secret Key Storage Solutions Is Low, Yet Counterfeiting Awareness Is High

Most participants are aware of the counterfeiting issue, yet the discussion of it inside and outside the company tends to be low for fear of damaging their brand. The topic is one best addressed at the most senior levels of the company and implies that suppliers must establish executive sales strategies. Twenty-four percent of participants had implemented some form of key storage prior to taking the survey, which was higher than anticipated. The percentage of participants who were not familiar with or had implemented or evaluated secret key storage was 49 percent (Figure 3). For some HIS Initiative advisers, this latter result was surprising, as they thought the percentage would be higher.

Seventy-three percent of participants indicated they were not aware that HIS could address their security needs. This

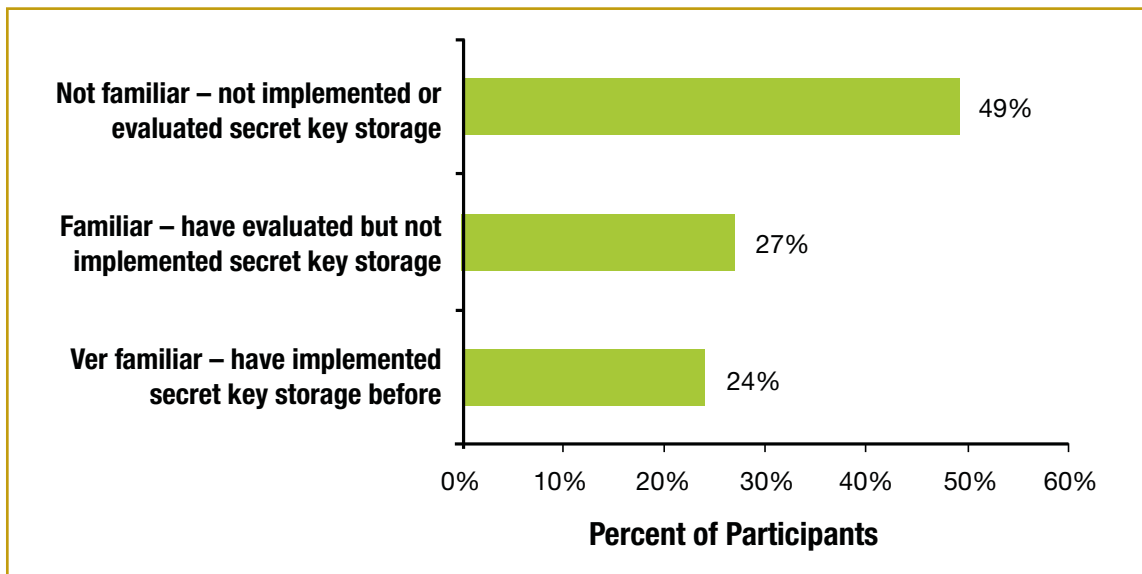


Figure 3. 49 percent of participants had not implemented or evaluated secret key storage prior to completing the survey, indicating an opportunity to increase market awareness.

result was more in line with the expectations of the HIS Initiative advisers.

Most participants were aware of the general issue of counterfeiting, and 58 percent of them agreed with the KPMG/AGMA study, which said that 10 percent of all high-tech products sold globally are counterfeit (Figure 4). However, the fact that 29 percent think it's much smaller than 10 percent was a surprise to some but not all of the HIS Initiative advisers. Another important result from the KPMG/AGMA study was that the No. 1 recommendation to prevent counterfeiting was to design-in and employ copy-resistant, anticounterfeit technologies in all products.

A surprising result was that participants equally felt that semiconductor (31 percent) and systems customers (32 percent) are responsible for preventing counterfeiting, cloning and theft-of-service. A possible explanation is that with 49 percent of participants not familiar with secret key

storage, they have not yet worked through the discussion with their customer or supplier. As the HIS Initiative advisers pointed out, in some early adoption markets such as smart cards, where security is a high priority, roles are clear and semiconductor companies are providing secret key storage.

### **Cost Is the Top Barrier That Must Be Addressed to Increase the Adoption of Secret Key Storage and HIS**

Cost of ownership and reliability garnered the highest ratings among participants as the most important attributes in a hardware security or secret key storage solution. While they were the top attributes, availability and technology independence were also clearly important. Seventy percent of participants rated availability with a 4 or 5 – the most important ratings. Technology independence garnered a 4 or 5 rating by 47 percent of participants. The sentiment that all these attributes are important was further supported by the responses to the question, “How would you assess the security of HIS solutions?”, with 31 percent of participants indicating that all of the techniques listed would be part of the assessment of HIS security.

A follow-on question to Figure 1 explored the reasons why participants had not designed-in secret key storage even though it was relevant to their product. Thirty-eight percent of participants indicated they were not familiar with the options or were not clear on the return on investment (ROI) that illustrates the need for more market education.

Twenty-eight percent of participants who had used key storage but were not satisfied indicated cost of ownership as the most important attribute to improve.

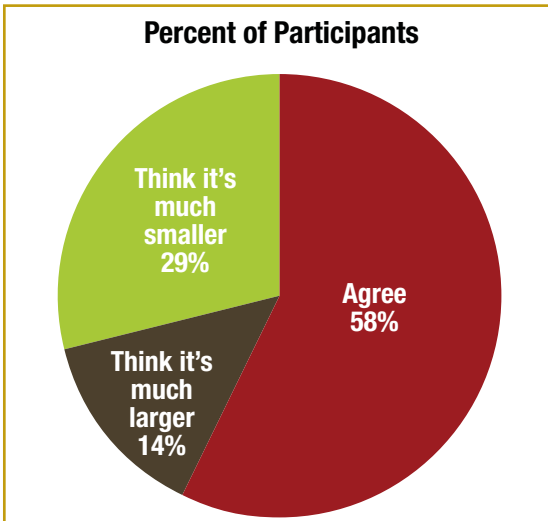


Figure 4. Most participants were aware of the general issue of counterfeiting, and 58% said they agreed with the assessment that 10% of all high-tech products sold globally are counterfeit.

Reliability, with 21 percent, was a relevant result and consistent with previous results.

In anticipation of the cost concern, a question was included within the survey to get a better idea of what level of cost fabless companies could absorb for adding HIS. A positive response was given, with 46 percent of participants indicating they could absorb up to 1 percent of their product cost for implementing HIS. As the HIS Initiative advisers pointed out, given the nature of negotiations, this survey response may reflect the participants' views on the starting point for the negotiation rather than the ending point. Regardless, 66 percent reflected a willingness to pay for HIS.

## Summary

In conclusion, the survey results provide valuable insight into the perceptions of implementing secret key storage and HIS among fabless companies. As suspected, the survey confirms that awareness of secret key storage is low, while the need is high and varies by customer application. Awareness of the overall issue among participants is good, but this topic should be addressed further at the senior management level. While cost is the top barrier that must be addressed to increase the adoption of secret key storage and HIS, other barriers must also be dealt with simultaneously to secure adoption. The market would greatly benefit from more education on counterfeiting and ways to address it through design-in of technologies such as HIS.

## About GSA

GSA's mission is to accelerate the growth and increase the return on invested capital of the global semiconductor industry by fostering a more effective ecosystem through collaboration, integration and innovation. GSA identifies and articulates market opportunities, encourages and supports entrepre-

neurship, and provides members with comprehensive and unique market intelligence.

[www.gsaglobal.org](http://www.gsaglobal.org)

## About HIS Initiative

The HIS Initiative provides a forum for educational activities regarding a new hardware security approach known as hardware intrinsic security (HIS). The goals of the initiative are to validate the HIS approach by industry leaders, increase the education available and reduce the barriers to adoption of HIS solutions.

[www.hisinitiative.org](http://www.hisinitiative.org)

## About the Authors

### Chelsea Boone

Chelsea Boone serves as director of research at the Global Semiconductor Alliance and is responsible for all reports, publications, directories, surveys and business tools created and distributed by GSA. She also serves as executive director of the alliance's industry-leading journal, GSA Forum, and manages the activity of GSA's interest groups and working groups. Boone earned a B.S. in management with an emphasis in marketing from Brigham Young University's Marriott School of Management.

### Pim Tuyls

Dr. Pim Tuyls initiated work on physically unclonable functions (PUFs) within Philips Research in 2001. Since 2004, he has been a visiting professor at the COSIC institute of the Katholieke Universiteit Leuven. In May 2010, Dr. Tuyls became CEO of Intrinsic-ID. He holds numerous patents, has presented several papers relating to PUFs at leading security conferences, and co-authored the 2007 book "Security with Noisy Data." ■