



*HARDWARE INTRINSIC SECURITY:
FABLESS PERCEPTION AND
AWARENESS STUDY*

2010 HARDWARE INTRINSIC SECURITY USAGE SURVEY ANALYSIS

Conducted by



in Conjunction with



THE HIS INITIATIVE



EXECUTIVE SUMMARY

Purpose of Study

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 have estimated that 10% 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 reported 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), the Global Semiconductor Alliance (GSA) and the HIS Initiative collaborated in mid 2010 to determine perception and awareness of secret key storage and the new HIS approach. The collaboration resulted in an online survey—the HIS Usage Survey—conducted July-August 2010.

Key survey findings include:

- **The need for secret key storage in the semiconductor industry is strong.** 48% of survey participants indicated secret key storage is a feature or requirement today, and 47% indicated they need secret key storage in the next year.
- **Awareness of secret key storage techniques is low, while awareness of counterfeiting is high.** 49% of participants indicated they are not familiar with nor have evaluated or implemented secret key storage. 73% of participants were not aware of HIS as a solution to secret key storage prior to taking the survey. However, the need is validated as 58% of participants agreed with a statement within a KPMG study that 10% of all high-tech products sold are counterfeit.
- **Cost is the top barrier that must be addressed to increase the adoption of secret key storage and HIS, in particular.** Cost and reliability garnered the highest ratings among participants as the most important attributes in a hardware security or secret key storage solution. A very promising opportunity is to reduce costs through HIS adoption. When told it was possible to eliminate the need for on-chip non-volatile memory (NVM) with HIS, 86% of participants indicated they would at least be interested in learning more about HIS.

Methodology & Response Demographics

The HIS Initiative and GSA are concerned about the increasing threat of counterfeiting, cloning and theft-of-service to their members. New secret key storage approaches used to make IC devices unclonable have

come to market, including HIS. To gauge perceptions and awareness around counterfeiting, secret key storage and HIS, the HIS Initiative released a quantitative online survey through GSA. GSA surveyed respondents with various titles at fabless companies. GSA defines as fabless company as any semiconductor firm that outsources 75% or greater of its wafer manufacturing and sells silicon to an end customer. The survey garnered 59 valid, anonymous industry respondents.

The research for the report was conducted by the HIS Initiative and based on the anonymous survey results. The results were reviewed by the HIS Initiative advisors, and their input helped shape the analysis and conclusions. The advisors include:

Jan Willis, Calibra and HIS Initiative Facilitator
 Jan Schlossberg, Cisco
 Pim Tuyls, Intrinsic-ID
 John Walker, SiVenture
 Chiente Ho, TSMC

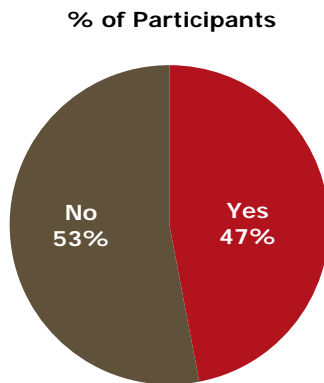
Hans Dekker, Irdeto
 Harmke de Groot, IMEC
 Christian Wiebus, NXP
 Patrick van de Steeg, Synopsys

ANALYSIS

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

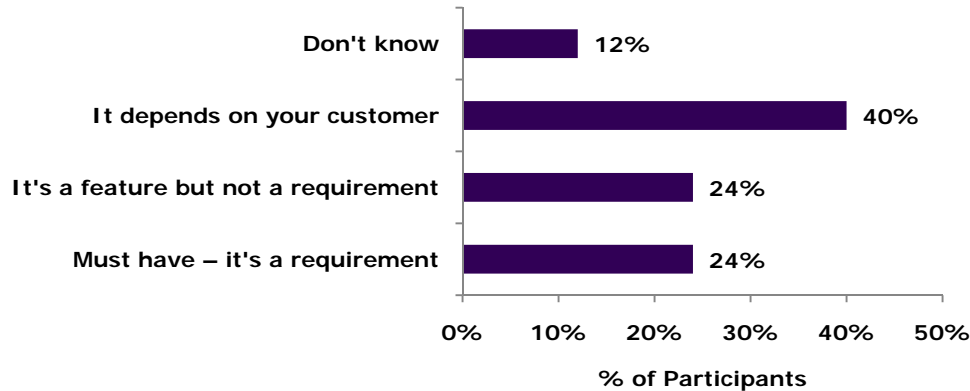
One of the most significant findings is that 47% of survey participants said they need secret key storage in the next year – 2011 (Figure 1). 48% of participants indicated secret key storage is currently a feature or requirement from their customers. An additional 40% indicated that the need for secret key storage is dependent on their customer (Figure 2). 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% selecting 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% and was followed closely by industrial, set-top box and military/aerospace (Figure 3).

Figure 1. Do you need secret key storage in the next year?



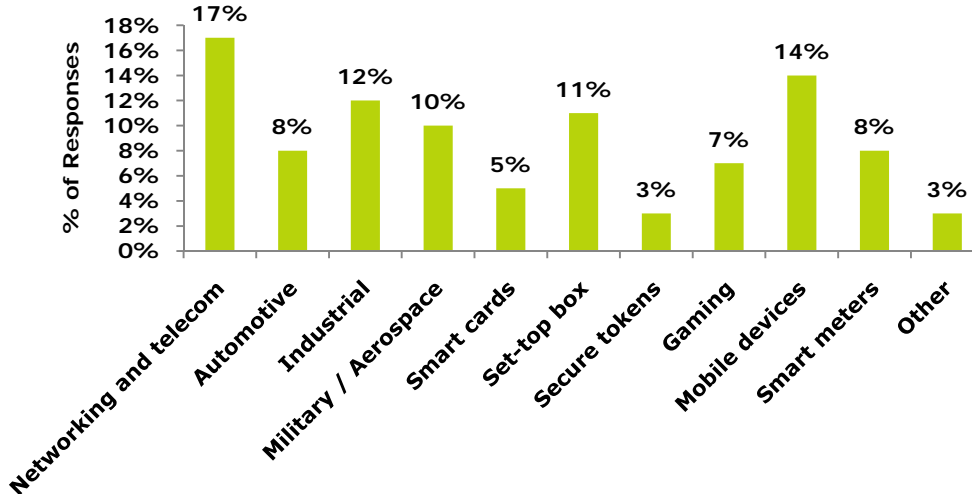
47% of participants indicated their need for secret key storage in 2011.

Figure 2. How would you characterize your need for secret key storage or hardware security in your product(s) or your customers' products(s)? (choose one)



48% of participants indicated that secret key storage is a feature or requirement today in 2010, with an additional 40% indicating that it depends on the customer.

Figure 3. For those who have indicated that you will need secret key storage in 2011, for what market applications will you be implementing secret key storage? (choose as many as apply)

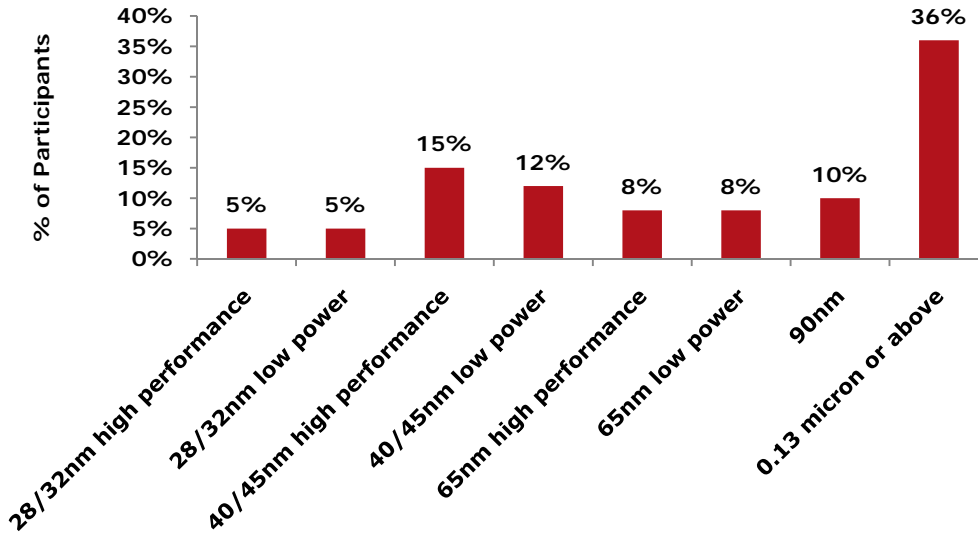


Networking and telecom was the highest ranking market application for implementation of secret key storage in 2011. Market segments with higher margins attract counterfeiters and have a more urgent need for secret key storage.

When asked to identify the most advanced technology node in use at their company today, 62% of respondents indicated 65nm, 90nm or 130nm (or above) as their most advanced technology node (Figure 4). However, the relatively large number of small companies which responded to the HIS Usage Survey could be a possible explanation for the large percentage at mature nodes. The large percentage (36%) of respondents which selected 130nm (or above) further supports the results from GSA's Q3 2010 Wafer

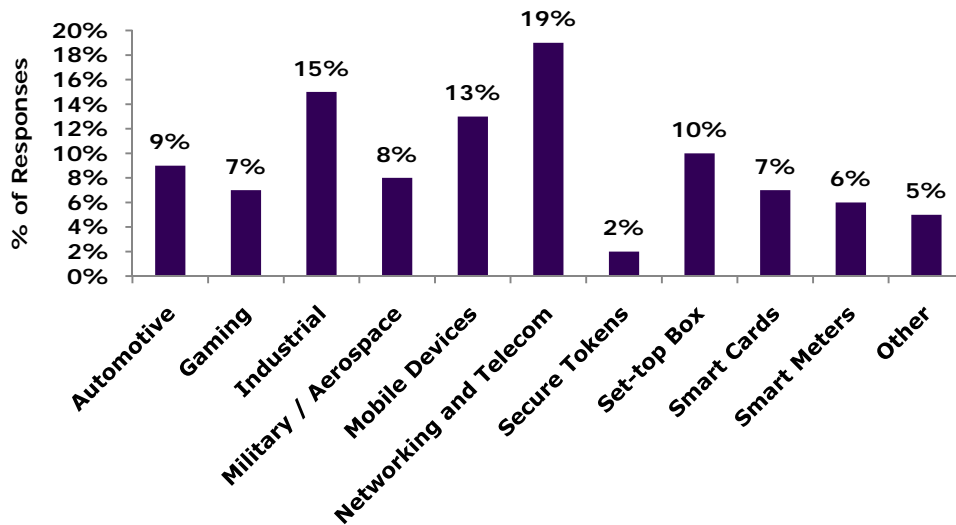
Fabrication & Back-End Pricing Survey which indicated that most chip companies believe the 180nm technology node will maintain or increase their market share in the future.

Figure 4. What is the most advanced technology node that your company is using in production or prototyping today (2010)? (choose one)



36% of participants are still at 130nm (or above), and 62% are using 65nm or larger geometries.

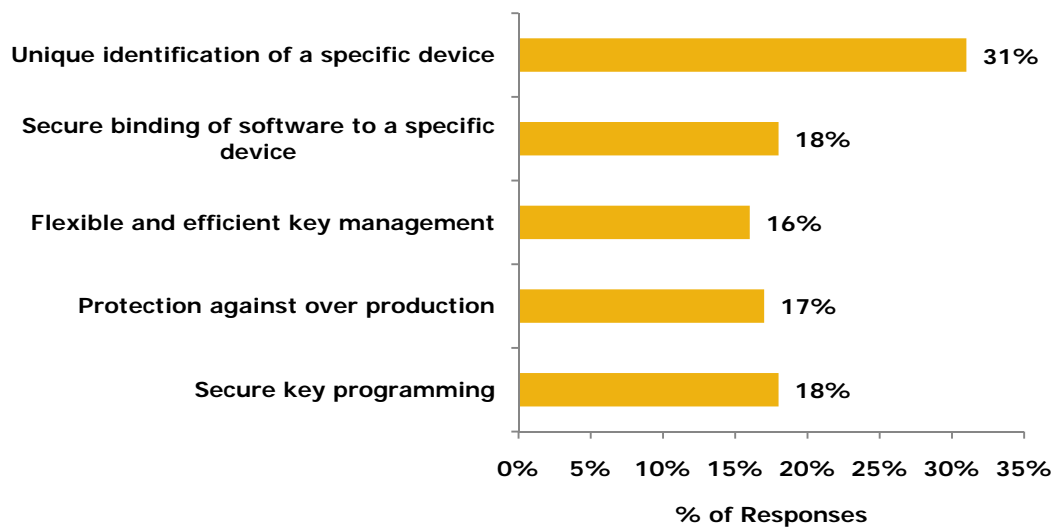
Figure 5. What end market segments do you participate in? (choose as many as apply)



Response to the survey is voluntary, so it's likely that those who responded are more interested in secret key storage, and it comes as no surprise that the results are similar to Figure 3.

Unique identification of a specific device ranked as the top driver for secret key storage adoption with 31% of responses. Secure binding of software to a specific device and secure key programming were tied for second with 18% of responses (Figure 6). This result was slightly surprising to a few HIS Initiative advisors who had anticipated secure binding of software to a specific device to be the number one response. This result possibly reflects the high degree of outsourcing by GSA members and that most participants were semiconductor companies and not systems companies.

Figure 6. Which of the following items are so important to you that you would address them if an appropriate hardware security solution existed? (choose as many as apply)



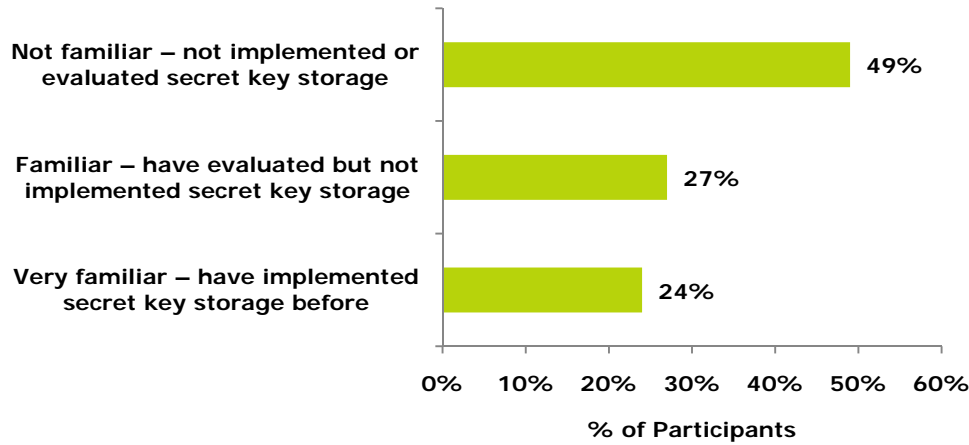
Unique identification of a specific device is the dominant reason given by survey participants for adopting secret key storage.

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. 24% 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% (Figure 7). For some HIS Initiative advisors, this latter result was surprising as they thought the percentage would be higher.

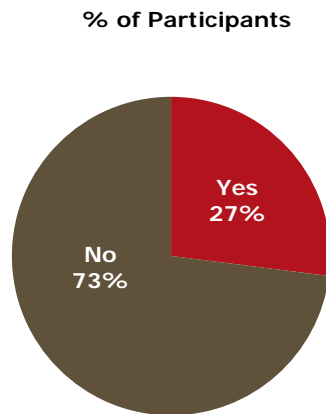
After answering the question seen in Figure 6, 73% of participants then indicated they were not aware that HIS could address their security needs (Figure 8). This result was more in line with the expectations of the HIS Initiative advisors.

Figure 7. How would you rate your understanding of what solutions are available today for secret key storage? (choose one)



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

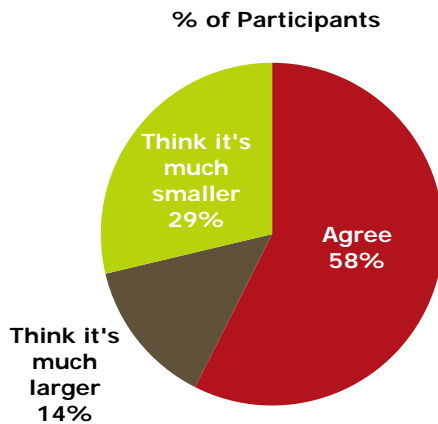
Figure 8. Prior to this survey, were you aware that HIS can address the issues in Figure 6?



An even greater market awareness opportunity exists for HIS, with 73% of participants not aware of HIS prior to taking this survey.

Most participants were aware of the general issue of counterfeiting, and 58% of them agreed with the KPMG and Alliance for Gray Market and Counterfeit Abatement (AGMA) study which said that 10% of all high-tech products sold globally are counterfeit (Figure 9). However, the fact that 29% think it's much smaller than 10% was a surprise to some but not all the HIS Initiative advisors. Another important result from the KPMG/AGMA study was that the number one recommendation to prevent counterfeiting was to design-in and employ copy-resistant, anti-counterfeit technologies in all products.

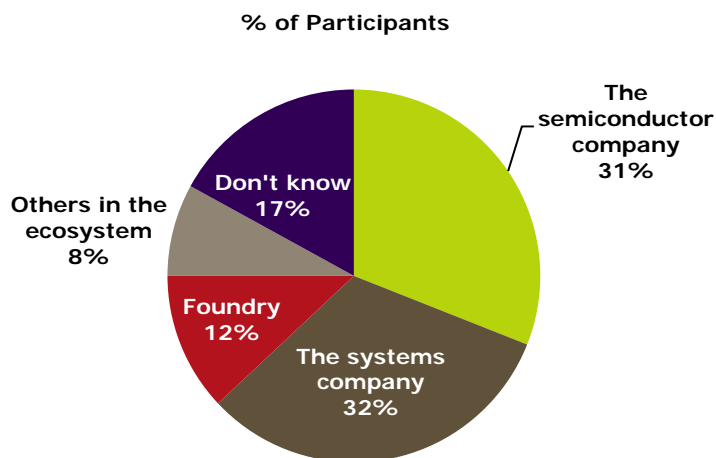
Figure 9. According to a study from KPMG and Alliances for Gray Market and Counterfeit Abatement, 10% of all high-tech products sold globally are counterfeit. What do you think? (choose one)



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.

A surprising result was that participants equally felt that semiconductor (31%) and systems customers (32%) are responsible for preventing counterfeiting, cloning and theft-of-service (Figure 10). A possible explanation is that with 49% of participants not familiar with secret key storage (Figure 7), they have not yet worked through the discussion with their customer or supplier. As the HIS Initiative advisors 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.

Figure 10. Who do you believe is responsible for preventing counterfeiting, including cloning and over production of systems as well as theft-of-service? (choose one)

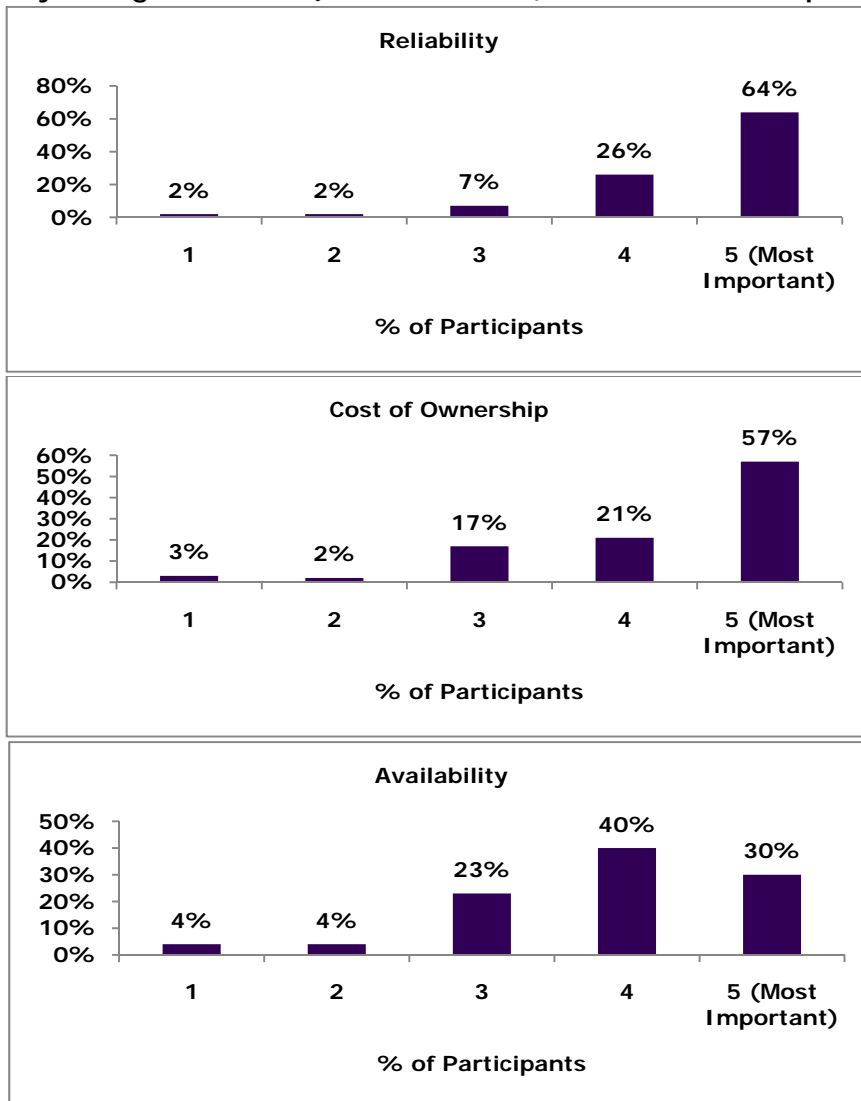


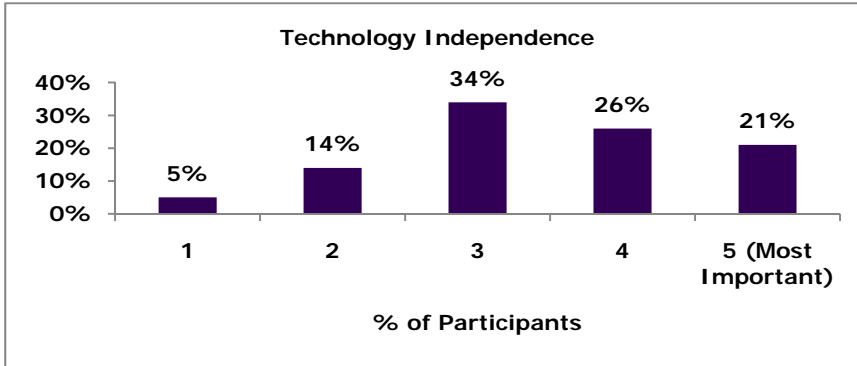
Participants were divided on whether the semiconductor or systems company is responsible for security.

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 (Figure 11). While they were the top attributes, availability and technology independence were also clearly important. 70% of participants rated availability with a 4 or 5—the most important ratings. Technology independence garnered a 4 or 5 rating by 47% of participants. The sentiment that all these attributes are important was further supported by the responses to the question seen in Figure 12, with 31% of participants indicating that all of the techniques listed would be part of the assessment of HIS security.

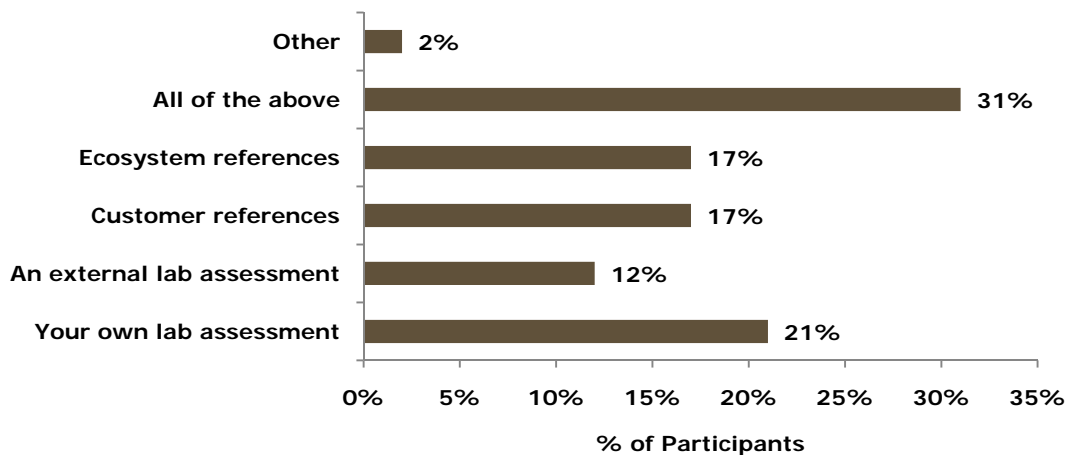
Figure 11. Please rate the importance of each of these attributes in a hardware security or secret key storage solution. (rate from 1 to 5, where 5 = most important)





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. Availability and technology independence were also clearly important.

Figure 12. How would you assess the security of a HIS solutions? (choose one)

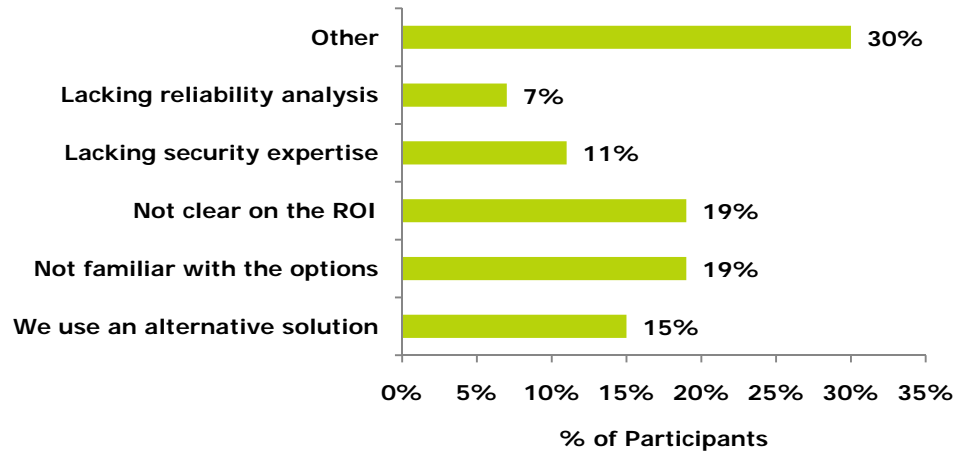


31% of participants indicated that all the techniques listed would be part of the assessment of HIS security.

A follow-on question to Figure 3 explored the reasons why participants had not designed-in secret key storage even though it was relevant to their product. 38% of participants indicated they were not familiar with the options or clear on the return on investment (ROI) which illustrates the need for more market education (Figure 13).

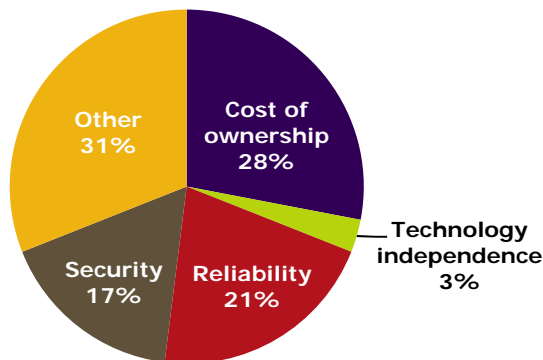
28% of participants who had used key storage but were not satisfied indicated cost of ownership as the most important attribute to improve (Figure 14). Reliability with 21% was a relevant result and consistent with the attributes given in Figure 11.

Figure 13. If secret key storage was relevant to your product but not designed-in, what was the main reason? (choose one)



With a combined total of 38% of participants saying they are not clear on the ROI or not familiar with the options of secret key storage, there is a clear need for market education.

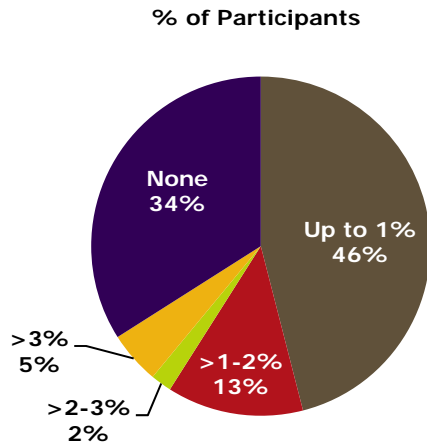
Figure 14. If you have used key storage and were not satisfied, what would be the most important attribute to improve? (choose one)



Cost of ownership is an important factor in satisfying customers.

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% of participants indicating they could absorb up to 1% of their product cost for implementing HIS (Figure 15). As the HIS Initiative advisors 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% reflected a willingness to pay for HIS.

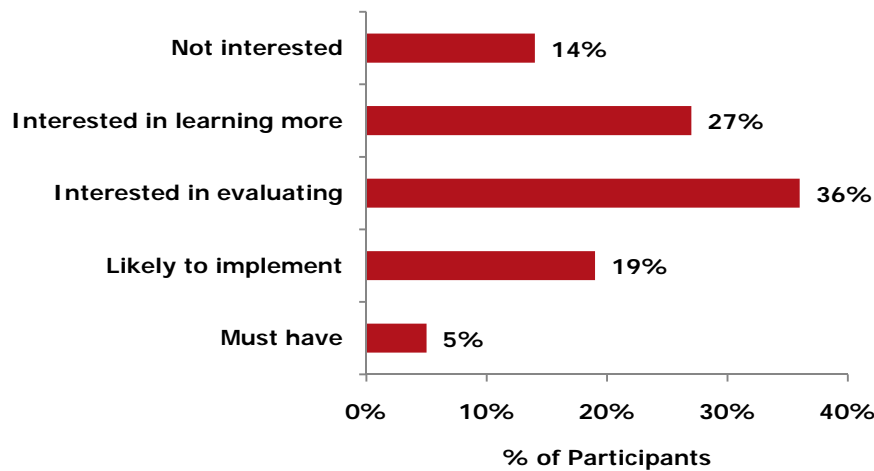
Figure 15. How much could you absorb in your product cost to implementing HIS which doesn't require the key to be stored on-chip and hence is more secure? (choose one)



A positive response was given for how many participants would pay to implement HIS, with 46% saying up to 1%.

A hypothesis was tested given that HIS does not require on-chip NVM. When asked to rate their interest in HIS, knowing that they could eliminate the need for on-chip NVM by using HIS, 87% of participants indicated they would at least be interested in learning more about HIS (Figure 16). If NVM is required to meet some other requirement on-chip, then HIS can't provide this benefit. But should NVM be present only for secret key storage, then HIS clearly brings a strong value proposition in this case.

Figure 16. If a HIS approach to key storage could enable you to eliminate the need for on-chip NVM, how would you rate your interest in a HIS solution? (choose one)



The sum of the interest by participants tallied 87%, which is a significant increase and clear market opportunity where it applies.



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. For applications where NVM is being used for key storage only, there is a very good opportunity to improve the customer's cost of ownership using HIS. 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

The Global Semiconductor Alliance (GSA) mission is to accelerate the growth and increase the return on invested capital of the global semiconductor industry by fostering a more effective fabless ecosystem through collaboration, integration and innovation. It addresses the challenges within the supply chain including IP, EDA/design, wafer manufacturing, test and packaging to enable industry-wide solutions. Providing a platform for meaningful global collaboration, the Alliance identifies and articulates market opportunities, encourages and supports entrepreneurship, and provides members with comprehensive and unique market intelligence. Members include companies throughout the supply chain representing 25 countries across the globe. 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). HIS technology provides a new level of hardware security utilizing the inherent uniqueness in each and every silicon chip. 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. Members, which span the semiconductor ecosystem, include: Cisco Systems, imec, Intrinsic-ID, Irdeto, NXP, SiVenture, Synopsys and TSMC. To find out more, please visit www.hisinitiative.org.

COPYRIGHT AND LEGAL DISCLAIMER

This publication is protected by United States copyright laws and international treaties, and is copyrighted by GSA. This document may not be reproduced or posted on another Web site beyond GSA and the HIS Initiative without the prior written consent of GSA. Unauthorized reproduction of this publication or any portion of it may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent necessary to protect the rights of the publisher.