Final

Annex 1: WSC Encryption Principles

Lisbon, 23 May 2013

WSC Encryption Principles

Background

The World Semiconductor Council (WSC)[1] recognizes that it is important to ensure that markets will be open and free from any discrimination. The competitiveness of companies and their products should be the principal determinant of industrial success and international trade. Governments and authorities should, therefore, ensure full intellectual property protection, full transparency of government policies and regulations, non-discrimination for foreign products in all markets and removal of unreasonable burdens on world commerce.

Semiconductors are overwhelmingly used as building blocks for computers, mobile phones, handheld devices and many other widely available commercial information and communications technology (ICT) products and systems. The functionality of semiconductors constantly evolves in order to meet consumer demands, which have increasingly called for product features such as encryption that better protect security and privacy in and across a variety of ICT products and systems. The use of encryption thus is not limited to government and military applications but has become widespread, given its ability to help safeguard the integrity and confidentiality of information. As a result, the great majority of applications of encryption involve every day commercial products which are commonly used and traded in the global marketplace.

Indeed, nearly all ICT products contain encryption to prevent data loss, ensure security and integrity of data (e.g. personal data or in communication) and allow for valuable commercial applications such as mobile payments, e-health, e-passports. Although encryption is a secondary feature for widely available ICT products such as garage door openers, mobile phones, ATM machines, internet browsers, DVD players and other common products, consumers demand it in their technological devices to ensure their communications are secure and private. Encryption is now part of the foundation of the internet and e-commerce developments. In many of these applications encryption functionality (besides other functions) is provided by semiconductors.

Regulations that directly or indirectly favor specific technologies, limit market access or lead to forced transfer of intellectual property stifle domestic innovation and, in the case of encryption, prevent access to the strongest available security technologies in the market place, resulting in less secure products. Both global collaboration and open markets for commercial

[1] The WSC represents global leaders in the manufacturing and design of semiconductors and is comprised of the Semiconductor Industry Associations in China, Chinese Taipei, Europe, Japan, Korea, the United States.

encryption technologies should therefore be strongly encouraged as they inherently promote more secure and innovative ICT products.

Very few countries have regulations governing the importation and use of encryption. The global trend is toward further de-regulation for mass marketed or widely available IT items in recognition of their widespread use and very limited value in regulating the commercial market.

Encryption Principles

Encryption regulations shall not be used for the purposes of limiting market access for foreign products. To prevent unnecessary restrictions on trade, products with cryptographic capabilities that are, or will be, widely available and deployed -- whether as a result of sales through normal or common retail channels, OEM sales or other means of distribution -- should not be regulated as a general matter except in narrow and justifiable circumstances (e.g., resulting out of international conventions such as export controls to prevent proliferation of munitions and weapons of mass destruction to targeted countries or targeted end users). The WSC Principles make it clear that generally there should be no regulation of cryptographic capabilities in widely available products used in the domestic commercial market because mandating or favoring specific encryption technologies will reduce, not increase, security and also raise product costs.

To the extent that encryption regulation is necessary, the WSC recommends the following practices:

- Regulations should not directly or indirectly favor specific technologies, limit market access or lead to forced transfer of intellectual property to avoid stifling domestic innovation and, in the case of encryption, preventing access to the strongest available security technologies in the market place, resulting in less secure products.
- The WSC opposes technology mandates, including any that involve encryption use in domestic commercial markets, because (i) the significant impact they can have on society and our industry; and (ii) such mandates often become outdated as technologies quickly evolve, and thus they create significant interoperability issues.
- Any regulatory requirements must be applied on a non-discriminatory basis and in a manner no less favorable than that granted to domestic producers (consistent with Articles I and III of GATT 1994), and respect intellectual property rights (consistent with Articles 28 and 31 of TRIPS 1994).
- Global collaboration and open markets for commercial encryption technologies should be strongly encouraged as both inherently promote more secure and innovative ICT products.
- Regulatory procedures related to the notification, evaluation, approval, or licensing of goods containing encryption technology, and the process for exempting goods, should be transparent, predictable and consistent with international norms and practices. They should not impose unreasonable or burdensome requirements on such goods. JSTC shall discuss international norms and practices.

The WSC believes that adhering to these practices will allow innovation and the digital

economy to flourish, and ensure that the strongest available security technologies will prevail and be available in all the market places to the benefits of all users of commercial products.

Clarifications

In regard to the use of international standards, norms and practices as required by one of the WSC Encryption Principles, the WSC provides the following clarification and statement:

- Definition of International

  The term international as a word means involvement of, interaction between or encompassing more than one nation, or generally reaching beyond national boundaries. For example, international law, which is applied by more than one country over the world, and international language which is a language spoken by residents of more than one country.

- International Standards

  International standards are standards developed by international standards organizations, which are open to all Members of the World Trade Organization or to most countries of the world. Notable examples of international standards bodies are the International Organization for Standardization (ISO) or the International Electrotechnical Commission (IEC). WSC supports and calls upon government authorities to follow the principles and procedures which have been decided by the WTO Technical Barriers to Trade Committee,[2] when international standards are elaborated by its members.

Examples of security related international standards, norms and practices are:

- Common Criteria (international standard). The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification.

- All testing laboratories must comply with ISO 17025, and certification bodies will normally be approved against either ISO/IEC Guide 65 or BS EN 45011.

- Mutual Recognition Agreement (Plurilateral agreement). As well as the Common Criteria standard, there is also a sub-treaty level Common Criteria MRA (Mutual Recognition Agreement), whereby each party thereto recognizes evaluations against the Common Criteria standard done by other parties. Originally signed in 1998 by Canada, France, Germany, the United Kingdom and the United States, Australia and New Zealand joined 1999, followed by Finland, Greece, Israel, Italy, the Netherlands, Norway and Spain in 2000. The Agreement has since been renamed Common Criteria Recognition Arrangement (CCRA) and membership continues to expand.

The WSC Encryption Principles strongly encourage the use of global or international standards, including normative algorithms, as essential to avoid fracturing the global digital infrastructure and creating unnecessary obstacles to trade. Because security functions are

[2] Source: Second Triennial Review of the Operation and Implementation of the Agreement on Technical Barriers to Trade, Annex 4, G/TBT/g, WTO Committee on Technical Barriers to Trade (13th November 2000)

growing in global ICT products and applications, interoperability has become more critical and thus international security standards such as Common Criteria for Information Technology Security Evaluation will increase in importance.

These security standards often define encryption functions for protection of information and data, as well as specify cryptographic algorithms that are developed or identified for the target application areas. Using standard cryptography as part of common protocols and specifying encryption algorithms to be used (along with making provisions for handling key management, etc.), enables an infrastructure to achieve global interoperability between security functions in products and systems. Whenever possible, the WSC will continue to support greater adoption of international security standards, rather than and instead of technology mandates.

General WSC Recommendations to Governments and Authorities

WSC encourages governments and authorities to advocate for transparency in any additional regulatory developments concerning the use of encryption in domestic commercial markets. Such transparency should include information on proposed testing and conformity assessments related to those regulatory developments. Testing and conformity assessments can create significant market barriers if they are not transparent, non-discriminatory, fully protective of intellectual property rights, based on international standards and done by qualified independent laboratories.

The availability of relevant information gives governments and authorities an option to weigh in on and shape the direction of potential regulatory measures and any implementing rules concerning encryption, which could impact trade in semiconductors and contradict WSC Principles, before those measures and rules are finalized. Indeed, as we noted in the WSC Principles, "The WSC requests the governments and authorities to continue their efforts to ensure that all WTO members observe the principles set forth above." Governments and authorities' efforts to increase transparency and help our industry ensure compliance with the WSC Principles going forward will help keep markets open and allow innovation and the digital economy to flourish.

Endorsement of WSC Encryption Principles by Governments and Authorities

The governments and authorities (GAMS) representing each of the six current WSC regions agreed to encourage all GAMS members and governments in general to observe the Encryption Principles that the WSC has developed since 2009 and to which GAMS members have committed at their annual government and authorities meeting on semiconductors in 2012. The GAMS acknowledged that the WSC Encryption Principles make it clear that in order to avoid negative impact on the industry's competitiveness, it is important to prevent unnecessary restrictions to trade, and that therefore, commercial products with cryptographic capabilities which are, or will be, widely available and deployed in the respective domestic markets should as a general matter not be regulated.

As recommended by the WSC, the GAMS also agreed to helping ensure open global markets that are free from discrimination by encouraging the adoption of international voluntary standards and norms, including algorithms, as essential to avoid fracturing the global digital infrastructure and creating unnecessary obstacles to trade. In the limited circumstances where

regulation may be necessary, the GAMS regions agreed to advocate for transparency and non-discrimination in any regulatory requirements, either in force or being developed concerning encryption in semiconductors used in domestic commercial markets, including the conformity assessment procedures used to demonstrate compliance with those requirements.

WSC Member Associations:

Semiconductor Industry Association in Europe:	*http://www.eeca.eu*
Semiconductor Industry Association in China:	*http://www.csia.net.cn*
Semiconductor Industry Association in Chinese Taipei:	*http://www.tsia.org.tw*
Semiconductor Industry Association in Japan:	*http://semicon.jeita.or.jp/en/*
Semiconductor Industry Association in Korea:	*http://www.ksia.or.kr*
Semiconductor Industry Association in the U.S.:	*http://www.semiconductors.org*

Find the full Joint Statement and more WSC information at : www.semiconductorcouncil.org