
RSA Data Security, Inc.

Answers to

Frequently Asked Questions

About Cryptography Export Laws



**THE KEYS TO
PRIVACY AND
AUTHENTICATION**

Copyright Notice

Copyright © 1996 by RSA Data Security, Inc. All rights reserved. No part of this work may be reproduced in any form or by any means—graphic, electronic or mechanical—including photocopying, recording, taping or storage in an information system, without the prior written consent of the copyright owner.

The RSA Public Key Cryptosystem is protected under U.S. Patent # 4,405,829.

BSAFE, TPEM, RC2, RC4 and RC5 are trademarks of RSA Data Security, Inc.

TABLE OF CONTENTS

| | |
|---|----|
| 1. Why is cryptography export-controlled? | 4 |
| 2. What's "strong" encryption? | 4 |
| 3. Which government agencies are involved in evaluating the exportability of encryption products? | 5 |
| 4. Which encryption algorithms are exportable? | 5 |
| 5. OK then, what types of crypto applications are "exportable"? | 6 |
| 6. I have developed a digital signature program. Do I have to fill out any paperwork before I ship overseas? | 7 |
| 7. How do I get permission to ship a product that uses "exportable" 40/512 crypto? ... | 8 |
| 8. What is a "test vector"? | 9 |
| 9. What types of applications are generally "not exportable"? | 9 |
| 10. How do I legally export a product which uses "strong" crypto? | 10 |
| 11. Where do I call to get all these forms? | 11 |
| 12. What's a "Manufacturing License Agreement"? | 11 |
| 13. I don't build crypto products, I just want to use them – and so do my overseas partners. An overseas subsidiary of my US-based company wants to buy a "strong" encryption product from a US manufacturer. Is this possible? | 12 |
| 14. I haven't begun development yet – but I want to develop a program that I'll be able to easily export. How do I design the application? What procedures do I have to go through before I start exporting? | 12 |
| 15. I'm building a secure telephone (or other encryption hardware). What are the guidelines for "strong" ("not exportable") hardware and "exportable" hardware? | 13 |
| 16. Cellular Digital Packet Data (CDPD) devices include RSA encryption technologies. Under what circumstances is CDPD exportable? | 13 |
| 17. I want to take my laptop on a business trip overseas – but I have a strong encryption program on my hard disk. What are the procedures? | 14 |
| 18. Some countries such as France, Hong Kong, and Singapore require "import" licenses. What are the procedures? | 14 |

1. Why is cryptography export-controlled?

Strong cryptography, in an enemy's hands, can be used for criminal purposes or even as a weapon of war. During wartime, the ability to intercept and decipher enemy communications is crucial. For that reason, strong cryptography is usually classified on the U.S. Munitions List as an export-controlled commodity, just like tanks and missiles. Cryptography is just one of many technologies which is covered by the ITAR (International Traffic in Arms Regulations).

2. What's "strong" encryption?

Government agencies consider "strong" encryption to describe systems which utilize asymmetric algorithms (like RSA) at key sizes over 512 bits, and symmetric algorithms (like DES, IDEA or RC5) at key sizes over 40 bits (in this FAQ, we'll call this "40/512 crypto"). Since government encryption policy is heavily influenced by the agencies responsible for gathering domestic and international intelligence (the FBI and the NSA, respectively) the government is compelled to balance the conflicting requirements of making strong cryptography available for commercial purposes — while still making it possible for those agencies to break those codes, if need be.

To most cryptographers, 40/512 cryptography is not considered "strong" at all — in fact, it is worth noting that RSA's mathematicians have considered 40/512 cryptography to be "commercially inadequate" for several years, and currently recommend that domestic customers utilize at least 80/768 cryptography.

Government agencies often prefer to use the terms "strategic" and "standard" to differentiate encryption systems. "Standard" refers to algorithms that have been drafted and selected as a federal standard — DES is the primary example. The government defines "strategic" as any algorithm which requires "excessive work factors" to successfully attack. Unfortunately, the government rarely publishes criteria for what it defines as "acceptable" or "excessive" work factors.

3. Which government agencies are involved in evaluating the exportability of encryption products?

Export applications for products containing cryptography are either handled by the Department of State or the Department of Commerce. But these evaluations are based upon the technical assessment of a third government organization — the Office of Export Control at the Department of Defense’s National Security Agency. NSA Export Control Officers often work directly with companies and review encryption products (in the context of the particular application for which the product will be used) in order to determine exportability.

4. Which encryption algorithms are exportable?

Products are commonly called “exportable” if they do not require an individual validated license prior to shipment to the customer or user. But it’s important to draw a distinction between an encryption application and an encryption algorithm. Since some algorithms feature adjustable key sizes (and hence adjustable levels of security), there is no published catalog of “exportable” algorithms. Therefore, regulations tend to focus on the application of these algorithms, using limited key sizes, inside of a software or hardware product.

5. OK then, what types of crypto applications are “exportable”?

Mass-market software applications which utilize RSA at 512 bits or less, and RC2 or RC4 at 40 bits or less, are currently considered “exportable”, and are eligible for special “fast-track” State Department reviews. Additionally, over the past few years, the State Department has adopted amendments within the ITAR (International Traffic in Arms Regulations) that have enabled applications whose functionality fits within any of 9 general categories to be regulated by the Department of Commerce, without a commodity jurisdiction request.

Under ITAR Section 121 Category XIII(b), you can usually export strong cryptography in the following types of applications:

- financial-specific applications
- fixed data compression or coding techniques
- decrypt-only licensing applications
- analog-only implementations
- personalized smart cards
- access control
- authentication
- entertainment decoders
- virus protection software

6. I have developed a digital signature program. Do I have to fill out any paperwork before I ship overseas?

Digital signature applications are one of the nine special categories of cryptography that automatically fall under the more relaxed Commerce regulations. No parameter restrictions apply, and therefore you can even create digital signature implementations that use RSA key sizes in excess of 512 bits! When developing a digital signature application using a reversible algorithm, such as RSA, the application should perform RSA on a hash of the message, not the message itself. Otherwise, the plaintext message must be transmitted with the “signature” appended. If the message is not transmitted with the signature, the NSA considers this quasi-encryption and State controls would apply.

In practice, however, prior to shipping overseas, a commodity classification request should be submitted to the Department of Commerce. This classification will indicate the specific export licensing requirements for the product. Experience has shown that Commerce personnel often request that a commodity jurisdiction (cj) request be obtained prior to issuance of the classification notice. In this event, contact the NSA Office of Export Control to coordinate the cj submission. It is not necessary to register with the Department of State prior to the submission of commodity jurisdiction requests or to export products controlled by Commerce.

7. How do I get permission to ship a product that uses "exportable" 40/512 crypto?

These products, which utilize RC2 or RC4 at 40 bits, and RSA at 512 bits, qualify for "fast-track" procedures which can get your application reviewed in about two weeks - that's lightspeed in Washington, D.C.! Fax a request for the Mass Market Commodity Jurisdiction Criteria and a test vector to the State Department at (703-875-6647). Your company will need to submit a commodity jurisdiction request letter (*see attachment*) - which includes

- a description of the software application
- the encryption algorithms and parameter sizes
- description of any pre / post processing on the data that is encrypted
- a completed test vector (see next FAQ question)
- product brochures

...to Sam Capino. Mr. Capino is the State Munitions Analyst responsible for CJ submissions, and he can be reached at (703) 875-7396.

Following the CJ review process, the State Department will transfer jurisdiction of the request to Commerce, and you will be notified. Then your company will need to submit a commodity classification request to the Commerce Department. The commodity classification documents the Department of Commerce export regulations for your particular application. Most mass market software is classified under ECCN 5D13A with the General Software Note (GSN) exemption allowing for general license (GTDU) applicability. Plainly speaking, this enables export to most countries without individual validated licenses. Some (obvious) country exceptions are Cuba, Iran, Iraq, Libya, North Korea, and Syria. After this, you may proceed with shipments without further interference from the government, aside from including some routine paperwork with your shipments, such as Shipper's Export Declarations (SEDs).

8. What is a “test vector”?

The “test vector” format, developed by the US Government, contains an example key, plaintext, and the ciphertext that is expected to be generated with that key, for both the RC2 and RC4 algorithms at 40 bits. The form also contains unique (indexed by serial number) test key and plaintext inputs. A developer of a 40/512 application would submit the test ciphertext output for verification. The purpose of the test vector is to demonstrate that the developer has an accurate 40 bit algorithm implementation. If the proposed test ciphertext checks, the application is transferred to Commerce. If not, the NSA Office of Export Control will contact the developer to resolve the situation. You can obtain test vectors from the State Department at 703/875-6647.

9. What types of applications are generally “not exportable”?

“Not exportable” doesn’t mean your product can *never* be shipped overseas — but it does mean that you have to get State Department approval for *each product shipment* - a long and sometimes tedious process. Applications of this type generally use RSA at key sizes greater than 512 bits, or DES at 56 bits, or RC2 or RC4 at key sizes greater than 40 bits. Other public-key and secret-key algorithms used at robust key sizes are similarly controlled. Effectively, the ITAR amendments mentioned above allow State to focus on cryptographic implementations that have a greater impact on technology transfer and national security concerns.

10. How do I legally export a product which uses “strong” crypto?

You must obtain permission from the State Department every time you wish to make a shipment of a product containing cryptography stronger than 40/512. As a manufacturer, to get permission to ship strong cryptography products, your company must

- 1) Contact the NSA’s Office of Defense Trade Controls and get a project manager assigned to your case (301-688-7834). Your project manager may request a copy of your crypto product, or at the very least, detailed documentation on the cryptography it contains.
- 2) Register with the U.S. State Department as a Munitions Manufacturer / Exporter by filling out the DSP-9 form. While an annual fee applies, it is possible to register for more than one year — a discount is offered for the five year registration periods.
- 3) Once given the “OK” by your NSA project manager, submit a DSP-5 (application for permanent export license) with the State Department.

You must file a DSP-5, and receive explicit approval of that DSP-5, for every “strong crypto” shipment you wish to make overseas, unless you submit a US based distribution arrangement or foreign distribution agreement. This paperwork is analogous to a blanket license; however, territory, end use, and end user restrictions will be necessary. Also, these agreements impose Department of State sales reporting requirements. NSA product evaluations, individual license requests, and agreements can be long processes, taking many weeks — even months — so it is prudent to consider these delays during your regular product planning.

Generally, your DSP-5 application will only be approved under the following circumstances:

- 1) Use of your product in financial applications overseas, or
- 2) Overseas branches or subsidiaries of US companies, or
- 3) Overseas partners of US companies involved in a joint venture

You may qualify for certain exceptions from these procedures. Your NSA project manager or an analyst from the Office of Defense Trade Controls can explain export licensing options for you.

11. Where do I call to get all these forms?

The following forms can be obtained by faxing a request to the State Department at (703-875-6647):

| | |
|--------|---------------------------------------|
| DSP-9 | State Registration Application, |
| DSP-5 | Permanent Export License Application, |
| DSP-73 | Temporary Export License Application. |

12. What's a "Manufacturing License Agreement?"

A manufacturing license agreement (MLA) is an arrangement between a US cryptographic supplier, a foreign developer and the State Department. The agreement defines the terms and conditions under which the US company can export encryption technology and components to a foreign developer for implementation and distribution abroad. An MLA is required in order for RSA to ship toolkits (such as BSAFE or TIPEM) to non-US companies.

13. I don't build crypto products, I just want to use them — and so do my overseas partners. An overseas subsidiary of my US-based company wants to buy a "strong" encryption product from a US manufacturer. Is this possible?

Foreign subsidiaries of your US-based company can usually get permission to purchase the same encryption products utilized at your domestic sites. You can even export strong encryption to your foreign contractor, given that the equipment is to be used to protect your proprietary information associated with joint venture development efforts. Your US office may need to gather purchase order information from the foreign branch or assemble supporting documentation on the end use application to facilitate license processing and approval. If this is an off-the-shelf application, sometimes the manufacturer will submit the licensing paperwork for you. If they won't, your company may qualify for an exemption from State on the registration issue. (Contact the General Information Desk 703-875-6644 and ask to be connected with the NSA Liaison Officer for Licensing Support.)

14. I haven't begun development yet — but I want to develop a program that I'll be able to easily export. How do I design the application? What procedures do I have to go through before I start exporting?

Since the US export policy on encryption is constantly evolving, no "cookbook recipes" on how to build a more exportable encryption application apply. As a part of the design process, it is suggested to contact the National Security Agency Office of Export Control (301-688-7834). Personnel from this organization can work with companies interested in developing applications for an international marketplace. For Commerce controlled commodities, contact the Office of Technical Information Support Division (202-482-4905). Whether the finished product is controlled under State or Commerce, it is important to remember that it is the responsibility of the manufacturer to follow proper procedures prior to any overseas shipments.

15. I'm building a secure telephone (or other encryption hardware). What are the guidelines for "strong" ("not exportable") hardware and "exportable" hardware?

Most encryption hardware that does not fit within one of the nine ITAR special categories remain State controlled commodities, regardless of key sizes or algorithms utilized. Here again, no cookbook recipes apply. Exporting encryption based upon a "strong" algorithm may be permitted under some restrictions. The primary restrictions are usually country limitations dictated by current Department of State political embargoes (e.g. Libya, Iraq, North Korea). To obtain a license, make sure that your company is registered as a munitions manufacturer (DSP-9) and fill out a DSP-5 form with the guidance of your NSA project manager.

16. Cellular Digital Packet Data (CDPD) devices include RSA encryption technologies. Under what circumstances is CDPD exportable?

The NSA's Office of Export Control reviews and evaluates Cellular Digital Packet Data (CDPD) handset units and modems built in accordance with industry standards. Contact them directly to obtain licensing instructions. Eventually, NSA will probably move CDPD handset device oversight to Commerce, with the oversight for the more complex base station devices remaining under State control. This method of regulating many-to-one (many user units to one control unit) equipment architectures is consistent with export controls on other broadcast devices, such as TV decoders and satellite uplinks.

17. I want to take my laptop on a business trip overseas — but I have a strong encryption program on my hard disk. What are the procedures?

State has recently adopted a “personal use exemption” which waives license requirements for personal use of your encryption software while on business travel. Individual licenses are usually not required, and you can just get on the plane and go.

18. Some countries such as France, Hong Kong, and Singapore require “import” licenses. What are the procedures?

Many countries use “import” licenses to pursue domestic policy goals. In some instances, countries use the technical information required for many “import licenses” to steer business toward local companies... other governments have been accused of using this same information for outright industrial espionage. Should you desire to do business in a country with such import restrictions, and you can accept the requirements for technical disclosure that government may impose, you should consult with export agencies or legal firms with multi-national experience in order to comply with all applicable regulations. RSA’s export assistance office can help you locate such a firm. Call them at 410/268-8033.



RSA Data Security, Inc.
100 Marine Parkway, Suite 500
Redwood City, CA 94065-1031

Tel: (415) 595-8782
Fax: (415) 595-1873

Internet: info@rsa.com
<http://www.rsa.com>