DEFINING A SAMPLE TEMPLATE FOR GOVERNMENTAL PROCUREMENTS OF CRYPTOGRAPHIC PRODUCTS

A Thesis Submitted to
the Graduate School of Engineering and Sciences of
İzmir Institute of Technology
in Partial Fulfillment of the Requirements for the Degree of

MASTER OF SCIENCE

in Computer Engineering

by
Levent TAŞ

July 2006
İZMİR

We approve the thesis of **Levent TAŞ**

Date of Signature

.... **July, 11th 2006**

Assoc. Prof. Ahmet Hasan KOLTUKSUZ, Ph.D.
Supervisor
Department of Computer Engineering
İzmir Institute of Technology

.... **July, 11th 2006**
Prof. Şaban EREN, Ph.D.
Department of Computer Engineering
Ege University

.... **July, 11th 2006**
Assist. Prof. Tuğkan TUĞLULAR, Ph.D.
Department of Computer Engineering
İzmir Institute of Technology

.... **July, 11th 2006**
Prof. Kayhan ERCİYEŞ, Ph.D.
Head of Department
İzmir Institute of Technology

..
Assoc. Prof. Semahat ÖZDEMİR, Ph.D.
Head of Graduate School

ABSTRACT

DEFINING A SAMPLE TEMPLATE FOR GOVERNMENTAL PROCUREMENTS OF CRYPTOGRAPHIC PRODUCTS

It is a well-known truth that nobody can easily find a law, act, directive, code or a publicly available technical specification which describe crytopgraphic-based security systems and/or cryptographic modules in Turkey. Besides that, from the international aspect, the only government released standarts take place in the **"Federal Information Standarts Publication (FIPS) 140-2"**, published by United States **"National Institute of Standarts and Technology (NIST)"** on May 25th, 2001 (which became the international standart after Final Commitee Document accepted as "**ISO/IEC 19790:2006"** on March 9th, 2006) which specifies the security requirements that should be satisfied by a cryptographic module.

Since the protection of sensitive and valuable (sometimes life-critical) data transfered via critical governmental cryptographic systems is very important and requires high confidentiality, the need for defining a sample template technical specification of those cryptographic systems is that much high.

The sample template specification which is made up in this study aims to be a starting point or initiative for preparing a cryptographic module specification in governmental procurements.

ÖZET

DEVLET KRİPTO İHALELERİ İÇİN ŞARTNAME TASLAĞI HAZIRLANMASI ÜZERİNE BİR ÇALIŞMA

Türkiye'de kriptografik-tabanlı güvenlik sistemleri ve/veya kriptografik modülleri tanımlayan bir kanun, yönetmelik, emir veya kamu kullanımına açık bir teknik şartnamenin kolaylıkla temin edilemeyeceği iyi bilinen bir gerçektir. Bunun yanında, uluslarası açıdan bakıldığında, hükümet seviyesinde bu konuda yayımlanmış tek standart, A.B.D. NIST (National Institute of Standarts and Technology) tarafından 25 Mayıs 2001 tarihinde yayımlanan (09 Mart 2006 tarihinden itibaren ISO/IEC 19790 olarak uluslararası nitelik kazanan) ve bir kriptografik modül tarafından karşılanması gereken güvenlik ihtiyaçlarını tanımlayan **"Federal Information Standarts Publication (FIPS) 140-2"** standardıdır.

Devlete ait kritik kriptografik sistemlerle aktarılan kritik ve değerli verinin korunması çok öneme haiz olduğundan, bahse konu kriptografik sistemleri tanımlayan örnek bir şablon şartnamenin tanımlanması da o denli önemlidir.

Bu çalışma kapsamında oluşturulan örnek şablon şartname, resmi kurum/kuruluşlar tarafından gerçekleştirilecek kriptografik sistem tedarikleri için bir başlangıç noktası ve insiyatif olmayı hedeflemektedir.

PREFACE

This thesis is based upon a research done during my graduate studies at the Department of Computer Engineering, İzmir Institute of Technology, Turkey. In this study it is aimed to compose and refine all accessible information to finally form a “Sample Template Technical Specification” for governmental cryptosystem procurements. This study also intends to be a motivative and initiative one for taking steps more rapidly of “Defining Cryptographic Module Requirements” in Turkey.

I would like to express my sincere gratitude to my supervisor Assoc. Prof. Ahmet Hasan KOLTUKSUZ, Ph.D., for his advise and unique support during all the study long. And I also would like to thank the staff at the Graduate School of Engineering & Sciences and Office of the Registrar of Izmir Institute of Technology.

Finally, I wish to express my greatest thanks to my family and to my colleagues, who have supported me.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standart
ANSI	American National Standarts Instıtute
API	Application Program Interface
BAN	Cryptographic Protocol Logic devised by Burrows, Abadi and Needham
CBC	Cipher Block Chaining
CC	Common Criteria
CCEIS	Chief of Communications Electronics and Information Systems
CMT	Cryptographic Module Testing
CMVP	Cryptographic Module Validation Program
COCOM	Coordinating Commitee for Multilateral Export Controls
COMSEC	Communication Security
COTS	Commercial of The Shelf
CRT	Cathode Ray Tube
CSE	Communications Security Establishment of the Government of Canada
CSP	Critical Security Parameter
DEMA	Differential Electromagnetic Analysis
DES	Data Encryption Standart
DPA	Differential Power Analysis
DTR	Derived Test Requirements
EAL	Common Criteria Evaluation Assurance Level
EFP	Environmental Failure Protection
EFT	Environmental Failure Testing
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FAQs	Frequently Asked Questions
FDR	Failures-Divergence Refinement Model Checker
FIPS	Federal Information Processing Standart
FIPS PUB	FIPS Publication

GNY	Cryptographic Protocol Logic devised by Gong, Needham and Yahalom
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IPSEC	IP Security Protocol
ISO	International Organization for Standartization
MOD	Ministry of Defense
MOFA	Ministry of Foreign Affairs
NIST	National Institute of Standarts and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
OECD	Organisation for Economic Co-operation and Development
PALCAN	Program for The Accreditation of Laboratories-Canada
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PKI	Public Key Infrastructure
SCA	Side Channel Attack
SCC	Standarts Council of Canada
SEMA	Simple Electromagnetic Analysis
SPA	Simple Power Analysis
SSL/TLS	Secure Socket Layer/Transport Layer Security
SvO	Cryptographic Protocol Logic devised by Syverson and van Oorschot
TEMPEST	A name referring to the investigation, study, and control of unintentional compromising emanations from telecommunications and automated information systems equipment.
TÜBİTAK/UEKAE	Türkiye Bilimsel Araştırma Kurumu/ Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
URL	Uniform Resource Locator
WTLS	Wireless Transport Layer Security

CHAPTER 1

INTRODUCTION

1.1. Importance of The Study

You may not be able to see the end of the road clearly, if you travel on the cryptography highway. And nobody is being expected to help you. None of the crypto station sells a road map. The topic is always confidential and also not shareware. Retrospective studies have no sense, since none of the related works has one-to-one similarity with the one we have. And especially in Turkey, no publicly available study or information can be readily found.

Besides all above, in many of the governmental organizations in Turkey, there is an increasing demand for using cryptographic modules in transmitting/transfering their sensitive data via computer or telecommunication systems. Although most of these organizations use COTS (Commercial Off The Shelf) products in their private networks or intranets depending on the level of importance of their data, those COTS cryptographic products should better employed only in non-critical or less sensitive data transmits/transfers. In addition, since the capabilities (encryption power) of these COTS cryptographic systems are definite and limited, there is no need to prepare a technical specification to describe the minimum standarts and obligations.

But, if our concern will be the critical cryptographic systems (sometimes life-critical) which is subject to the very sensitive data like military data and high level political data, then we can not use neither, ordinary **"COTS Cryptographic Products"** commercially available to any one who pays the Money, nor "weak crypto" that can easily be imported.

In addition to that, COCOM **(Coordinating Commitee for Multilateral Export Controls)** Treaty (Turkey was a cooperating country), and the succesor Wassenaar Agreement (Turkey signed), which also have been regulating the export of cryptographic systems (hardware, software etc.), have a main goal **"to prevent cryptography from being exported to dangerous countries like Libya, Iraq, Iran and North Korea"** (WEB_1 2006). And since nobody can not guess the future of international political situation and the position of our country in that arena, we had better support **"the national cryptology initiative"** and the implementation of cryptographic systems/modules by national organizations or firms.

Shortly, the demand for using cryptographic systems in both commercial and governmental institutions are increasing geometrically. And this is followed by procurement and by the technical specification/description needs and so on. So, this study is a unpretentious candidate to be a initiative and motivative one for the future work of "cryptographic module requirements".

1.2. Problem Description

Due to the existence of following problems, **"it is intended to work on defining a sample template technical specification which might be used for the procurement of cryptographic modules/systems (protecting sensitive and valuable data) by governmental organizations in Turkey":**

a. Turkey, like most countries, leaves cryptography as yet unregulated or partially regulated.

b. Failing international consensus after COCOM, Wassenaar Arrangement and OECD Principles, countries are thinking of taking steps on their own, driven by a growing concern for criminal crypto use (WEB_1 2006).

c. In Turkey, the **"cryptology"** is expected to be under the control of **"Kriptoloji Dairesi Başkanlığı"** with respect to the **"draft"** act **"Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı"** (Başbakanlık 2000) and the regulations mentioned in the draft have no details to have an idea for the future work on the cryptography and cryptographic systems, and also on the specifications of cryptographic modules naturally.

d. Even though **FIPS 140-2 of NIST** and the "**ISO/IEC 19790:2006",** have been accepted as the international standarts on **"Cryptographic Module Requirements"** building to the FIPS 140-2 or ISO/IEC 19790:2006 standards is quite complicated. According to NIST, 48% of cryptographic modules submitted by new applicants and 20% of returning applicant modules contain security flaws. **"A full 30% of algorithms tested by NIST do not conform to the FIPS Standard"** (WEB_2 2006).

1.3. Solution Strategy

To reach to the aim of the study and to form an optimum template specification as a proposed solution of the study, we successively needed to;

- survey the international legal issues and legal issues in force in Turkey about the topic,
- review whole methodology of FIPS 140-2 (or ISO/IEC 19790:2006) item by item,
- review CMVP as a sub-topic for FIPS 140-2,
- analyze the formerly used technical specifications of cryptographic modules for governmental organizations procurements and compare them with FIPS 140-2 (or ISO/IEC 19790:2006),
- review all related works which are limited (due to the confidentiality of the topic) numbers of white papers, articles and graduate theses,
- evaluate and modify (if necessary) FIPS 140-2 context with respect to the related work and comparison conclusions,

- set up a sample template technical specification (in Turkish) and template matrix as an appendix to the study which consists of essential items (in text) needed for a technical specification of basic cryptographic module under the light of modified FIPS 140-2 context.

1.4. The Appendices

The CD medium have been preferred due to lengthy nature of the outcomes of this research. Those five different products of this thesis come with the CD can be found on the inside of the back cover.

CHAPTER 2

LEGAL ISSUES IN CRYPTOGRAPHY

2.1. International Conjuncture

The export of cryptography has long been restricted. Evidently, governments have wanted to avoid strong cryptography from falling into the hands of foreign powers, which would have thwarted their ability to do the intelligence work. Cryptography has long been regarded as a weapon, and it is still featuring on lists that control the export of munitions. The main international agreement on export controls, the treaty of COCOM, the Coordinating Committee for Multilateral Export Controls, was replaced by the Wassenaar Arrangement in 1996 (WEB_1 2006).

2.1.1. COCOM - The Coordinating Committee for Multilateral Export Controls

COCOM was an international organization for the mutual control of the export of strategic products and technical data from country members to defined destinations. It maintained, among others, the International Industrial List and the International Munitions List, regulating all kinds of cryptography. In 1989, COCOM decontrolled password and authentication-only cryptography. In 1991, COCOM decided to allow export of mass-market cryptographic software (including public-domain software). Most member countries of COCOM followed its regulations, but others, such as the United States, maintained separate regulations (WEB_1 2006).

The main goal of the COCOM regulations was to prevent cryptography from being exported to 'dangerous' countries – usually, the countries thought to maintain friendly ties with terrorists, such as Libya, Iraq, Iran, and North Korea. Exports to other countries were usually allowed, although states often required a license for these (WEB_1 2006).

2.1.2. Wassenaar Arrangement

COCOM was dissolved in March 1994. In 1995, 28 countries decided to establish a follow-up to COCOM, the **"Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies"**. The negotiations on the treaty were finished in July 1996, and the agreement was signed by 33 countries (now 40 countries). Turkey was one of the signers. The Wassenaar Arrangement controls the export of weapons and of dual-use goods, that is, goods that can be used both for a military and for a civil purpose; cryptography is such a dual-use good. The provisions are largely the same as COCOM regulations. The General Software Note (GSN) excepts mass-market and public-domain crypto software from the controls; five countries (Australia, France, New Zealand, Russia, and the US) deviate from the GSN and control the export of mass-market and public-domain crypto software. Export via the Internet does not seem to be covered by the regulations. The Wassenaar Arrangement was scheduled to be revised in late 1998 (WEB_1 2006).

In the Wassenaar Arrangement under DUAL-USE LIST-CATEGORY 4-COMPUTERS sub-title it is stated that; computers, related equipment and "software" performing cryptographic, cryptanalytic, certifiable multi-level security or certifiable user isolation functions, or which limit electromagnetic compatibility (EMC), must also be evaluated against the performance characteristics in Category 5, Part 2 ("Information Security") (WEB_4 2006).

And succesively under DUAL-USE LIST-CATEGORY 5-PART 2- “INFORMATION SECURITY" (WEB_4 2006), it is stated that; items that meet all of the following shall not be controlled:

- Generally available to the public by being sold, without restriction, from stock at retail selling points by means of any of the following:
  - Over-the-counter transactions.
  - Mail order transactions.
  - Electronic transactions or
  - Telephone call transactions;
- The cryptographic functionality that cannot easily be changed by the user.
- Designed for installation by the user without further substantial support by the supplier and
- Deleted.
- When necessary, details of the items are accessible and will be provided, upon request, to the appropriate authority in the exporter's country in order to ascertain compliance with conditions described in paragraphs a. to c. above.

And again DUAL-USE LIST-CATEGORY 5-PART 2- “INFORMATION SECURITY" (WEB_4 2006) does not control:

- Personalised smart cards where the cryptographic capability is restricted for use in equipment or systems excluded from control under following items or for general public-use applications where the cryptographic capability is not user-accessible and it is specially designed and limited to allow protection of personal data stored within.
- Receiving equipment for radio broadcast, pay television or similar restricted audience broadcast of the consumer type, without digital encryption except that exclusively used for sending the billing or programme-related information back to the broadcast providers.
- Equipment where the cryptographic capability is not user-accessible and which is specially designed and limited to allow any of the following:
  - Execution of copy-protected software.
  - Access to any of the following:

        - Copy-protected contents stored on read-only media.
        - Information stored in encrypted form on media (e.g. in connection with the protection of intellectual property rights) when the media is offered for sale in identical sets to the public;
    - Copying control of copyright protected audio/video data.
    - Encryption and/or decryption for protection of libraries, design attributes or associated data for the design of semiconductor devices or integrated circuits.
- Cryptographic equipment specially designed and limited for banking use or money transactions.
- Portable or mobile radiotelephones for civil use (e.g., for use with commercial civil cellular radiocommunications systems) that are not capable of end-to-end encryption.
- Cordless telephone equipment not capable of end-to-end encryption where the maximum effective range of unboosted cordless operation (i.e., a single, unrelayed hop between terminal and home basestation) is less than 400 meters according to the manufacturer's specifications.

2.1.3. OECD Crypto Policy

The OECD (Organisation for Economic Co-operation and Development) have developed “guidelines” for a crypto policy, after extensive discussions throughout 1996. The OECD started discussing and drafting policy guidelines in December 1995 with an Ad-hoc Meeting of Experts on Cryptography Policy. The guidelines were discussed and revised in several meetings in 1996, leading to the adoption of the “**Recommendation of the Council concerning Guidelines for Cryptography Policy”** on 27 March 1997. The guidelines are non-binding recommendations to Member governments, meaning that they are not part of international law. The guidelines provide principles which states should take into account and balance in developing a national crypto policy (WEB_1 2006).

The principles (WEB_1 2006) **are:**

- **Trust in cryptographic methods:** market forces and government regulation should foster user trust in cryptographic methods.
- **Choice of cryptographic methods:** users should have the right to choose any cryptographic method, subject to applicable law.
- **Market-driven development of cryptographic methods:** the market should determine the development and provision of cryptographic methods, including international standards.
- **Standards for cryptographic methods:** international and interoperable standards for cryptographic methods should be developed; national standards should be consistent with international ones.
- **Protection of privacy and personal data:** national cryptography policies and the implementation and use of cryptographic methods should respect the fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data.
- **Lawful access:** national cryptography policies may allow lawful access to plaintext or cryptographic keys.
- **Liability:** the liability of crypto users and of crypto service providers should be clearly stated.
- **International cooperation:** governments should cooperate to coordinate cryptography policies; governments should remove, or avoid creating, unjustified obstacles to trade.

The principles should be seen as "**interdependent and should be implemented as a whole so as to balance the various interests at stake. No principle should be implemented in isolation from the rest**" (WEB_1 2006). The balance basically has to be struck between the first five (crypto-friendly) principles and the sixth (policy-friendly) principle, lawful access. This crucial and most controversial principle reads: "National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible." Interestingly, the most crypto-friendly principle, free choice, was adapted at the final stage. Where the earlier version read that crypto users should have a right to choose any crypto method, this was extended with the restriction “subject to applicable law”, thus opening the door for a prohibition of cryptography (WEB_1 2006).

2.1.4. General Evaluation

The world wide survey of cryptography laws show that regulations differ widely. Some countries have implicitly prohibited cryptography (Russia, France). Others are looking at leaky solutions (in particular the US and the UK), but they face fierce opposition by their citizens. Moreover, other countries and the European Commission are wary of this approach. Some countries are looking at commanding people to decrypt as a solution. The Netherlands has enacted a law to that effect, which is currently under revision to enable the police to give a decryption command in more situations. Most countries leave cryptography as yet unregulated – if not by a conscious decision, then at least by a failure to develop a viable and broadly supported policy. The complexity of developing an acceptable crypto policy is also reflected in the international talks on the subject. After the failure of the OECD guidelines to steer international crypto policies, there is little hope that there will be an international or supranational agreement on addressing the crypto problem within the foreseeable future (WEB_1 2006).

Failing international consensus, countries are thinking of taking steps on their own, driven by a growing concern for criminal crypto use. However, most governments are confused over the direction of a policy, and they seem to be looking at other countries to see what the emerging international direction will be. So, there is a general impasse in the cryptocontroversy debate (WEB_1 2006).

2.2. Legal Situation of Cryptography in Turkey

In Turkey, the **"cryptology"** (and also cryptography) will be under the control of **"Kriptoloji Dairesi Başkanlığı"** with respect to the **"draft"** act **"Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı Taslağı"** (Başbakanlık 2000). And the regulations mentioned in the draft has no detail and far from explaining to have an idea for the future work on the cryptography and cryptographic systems, and also on the specifications of cryptographic modules naturally. The responsibilities of "Kriptoloji Dairesi Başkanlığı" (Başbakanlık 2000) with respect to the draft regulations are to:

- determine the need for cryptographic algorithms and inspect the production and establish the library.
- specify the principles and methods for the export and import of the cryptographic modules/information by coordinating with Turkish General Staff, Ministry of Foreign Affairs and other concerning government departments, and license.
- establish risk analysis and risk mitigation plans, to determine the acceptable risk.
- specify the criteria which should be provided by crypto centers and the methods and principles of inspections.
- approve the crypto center by evaluating the inspection reports.
- generate and distribute the cryptographic keys.
- license the official agencies for generating and distributing their own cryptographic keys in case of necessity.
- specify the utilization principles of cryptography in unclassified applications, and to encourage and inspect them.
- specify the crypto bookkeeping, operating, maintanence and repair methods for cryptographic modules and documentation.
- specify and take the required precautions against cryptographic violations.
- specify the certification and approval methods for every kind of cryptographic method and module.

- specify the principles and methods of cryptographic licensing for the personnel under the crypto services.

As mentioned above, there is no frame act in force on cryptology in Turkey. In the absence of execution in this area, some governmental institutions like Ministry of Defence (MoD) and Ministry of Foreign Affairs (MoFA) have taken the responsibilities.

Licensing the individuals and establishments who build or use cryptographic software and hardware which are required for defense systems, utilization of these systems and techniques for communication or transmission of any information/documentation, the request and specifications by administration and the rules that must be obeyed by the individuals and establishments, other execution principles and methods, all shall be explained in the specific directive that will be issued by MoD. Until that time all related activities shall be carried out by Turkish General Staff (TGS) (MSB 2003a). However, the procurement activities for cryptographic modules are stil carried out by MoD.

And for this kind of R&D required products one of the following "single source procurement" method is used with the countenance of Deputy MoD and approval of Minister of Defence (MSB 2006):

- The procurements for which the requirements are determined to be able to be provided only by factual or judicial single person.
- The procurements for which only a factual or judicial single person has a specific right for providing the requirements.

Cryptographic systems has defined under **"Obligatorily National Systems/ Technologies"** (for long term they should certainly be implemented or supplied in the country) and **"Critical Systems/ Technologies"** (for long term aiming to implement in the country or otherwise anticipated as joint production) (MSB 2003b).

For all kind of procurement activities (also for cryptographic modules) in MoD, **"M.S.B. Teknik Şartname Hizmetleri Yönergesi (MSY.: 202-12 (B))"** is the only valid legal document to be used.

2.3. Current Practice in Turkey

Government as being the only customer and TÜBİTAK-UEKAE as the only qualified vendor are currently carrying out all cryptographic activities including module design, implementation, production and testing. And TÜBİTAK/UEKAE proclaims (WEB_3 2006) that they carry out:

- cryptographic designs including key management and production protocols, symmetric keyed algorithms, cryptographic systems with public key, authentication protocols,
- tests and evaluations including cryptographic security tests, auditing with respect to IEEE, ANSI, ISO, FIPS standarts, NIST tests, COMSEC test and evaluations.
- EMC and TEMPEST tests.

CHAPTER 3

CRYPTOGRAPHIC MODULE SPECIFICATION

3.1. FIPS 140-2 – Security Requirements for Cryptographic Modules.

FIPS 140-2 is a NIST standard to be used by (US) Federal organizations when specifying cryptographic-based security systems to provide protection for sensitive or valuable data (maintaining the confidentiality and integrity of information). The FIPS 140 standard specifies the security requirements to be satisfied by a cryptographic module in four increasing, qualitative levels of security (Level 1 to 4, from low to high) as summarized in the following:

- **Security Level 1** provides the lowest level of security. It specifies basic security requirements for a cryptographic module (for software implementation only).
- **Security Level 2** improves the physical security of a Security Level 1 cryptographic module by adding the requirement for tamper evident coatings or seals, or for pick-resistant locks.
- **Security Level 3** requires enhanced physical security, attempting to prevent the intruder from gaining access to critical security parameters held within the module.
- **Security Level 4** provides the highest level of security. Level 4 physical security provides an envelope of protection around the cryptographic module to detect a penetration of the device from any direction (WEB_2 2006).

These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of the cryptographic module. These areas include the following: cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/ EMC); self tests; design assurance and mitigation of other attacks (WEB_2 2006).

The security requirements specified in FIPS 140-2 relate to the secure design and implementation of a cryptographic module. The requirements are derived from the following high-level functional security objectives for a cryptographic module:

- to employ and correctly implement the Approved security functions for the protection of sensitive information.
- to protect a cryptographic module from unauthorized operation or use.
- to prevent the unauthorized disclosure of the contents of the cryptographic module, including plaintext cryptographic keys and CSPs.
- to prevent the unauthorized and undetected modification of the cryptographic module and cryptographic algorithms, including the unauthorized modification, substitution, insertion, and deletion of cryptographic keys and CSPs.
- to provide indications of the operational state of the cryptographic module.
- to ensure that the cryptographic module performs properly when operating in an Approved mode of operation.
- to detect errors in the operation of the cryptographic module and to prevent the compromise of sensitive data and CSPs resulting from these errors.

The FIPS 140 standard is reexamined or reaffirmed in every five years. FIPS 140-1 standard specifies the security requirements to be satisfied by a cryptographic module used within a security system protecting unclassified information within computer and telecommunications systems (including voice systems). FIPS 140-2 superseded FIPS 140-1 in 2001 with technical modifications to address technological advances that had occurred since FIPS 140-1 had been issued (WEB_2 2006).

3.1.1. Challenges in FIPS 140-2 Validation

Moreover, building to the FIPS 140-2 standard is complicated. According to NIST, 48% of cryptographic modules submitted by new applicants and 20% of returning applicant modules contain security flaws. **"A full 30% of algorithms tested by NIST do not conform to the FIPS Standard"**. So vendors can spend time and money developing a solution that requires FIPS validation for the government market, then submit it to a testing process that can take months and afterwards learn that their solution is flawed and cannot be FIPS-Validated without improvements. Other challenges that point towards the need for an easier solution (WEB_2 2006) include:

- Increased need for in-house security expertise.
- Evolving FIPS standards that require continuous monitoring.
- Platform specificity of each FIPS validation.
- Requirement for re-validation when any feature changes are introduced into FIPS Validated product.

FIPS validation provides third-party verification that the secure technologies used by government agencies meet a predetermined security profile. NIST has accredited twelve (currently) third-party labs to test vendor products and technologies for FIPS validation but high demand combined with the thorough testing process results in lengthy waiting periods that can be up to a year (WEB_2 2006). This validation process is called "Cryptographic Module Validation Program" and will be mentioned in the following paragraphs.

At the beginning of this study FIPS 140-2 of NIST had been evaluated as "Final Committee Document" for ISO standard and ultimately has been accepted as ISO standart with "**ISO/IEC 19790:2006"** for **"Cryptographic Module Requirements"** on March 1, 2006.

3.2. CMVP - Cryptographic Module Validation Program.

To receive FIPS 140-2 validation, a cryptographic module must:

- Have a well-defined crypto boundary so that all sensitive security information remains within the cryptographic core of the product.

- Use at least one FIPS-approved algorithm with correct implementation and an intact crypto boundary.

The FIPS module must be validated through the **"Cryptographic Module Validation Program (CMVP)"** (WEB_2 2006). On July 17, 1995, the NIST established the CMVP that validates cryptographic modules to Federal Information Processing Standards (FIPS) 140-1 "**Security Requirements for Cryptographic Modules"**, and other FIPS cryptography based standards. The CMVP is a joint effort between NIST and the CSE of the Government of Canada. FIPS 140-2 was released on May 25, 2001 and superceded FIPS 140-1. However, agencies may continue to purchase, retain and use FIPS 140-1 validated products after May 25, 2002. Modules validated as conforming to FIPS 140-1 and FIPS 140-2 are accepted by the Federal Agencies of both countries for the protection of sensitive information. Vendors of cryptographic modules use independent, accredited Cryptographic Module Testing (CMT) laboratories to test their modules. The CMT laboratories use the "**Derived Test Requirements [DTR] for FIPS PUB 140-2, Security Requirements for Cryptographic Modules and Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program"** to test cryptographic modules against FIPS 140-2. NIST's Computer Security Division and CSE jointly serve as the Validation Authorities for the program, validating the test results. Shown below in Figure 1 is a summary of the CMV process (WEB_5 2006):

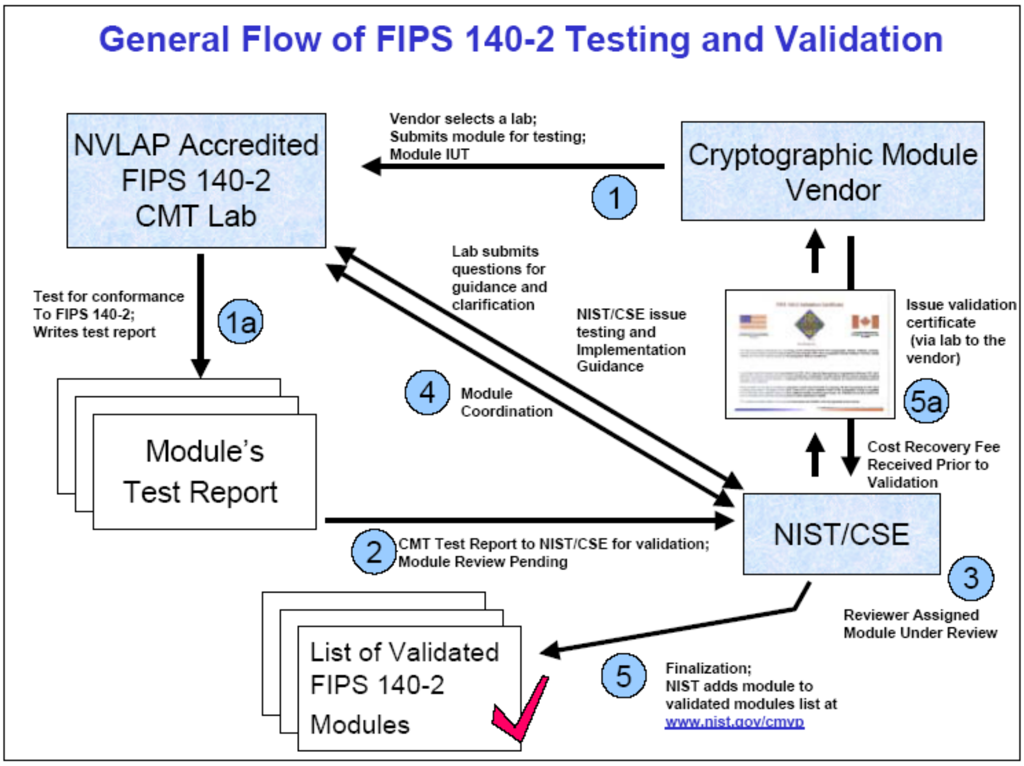

General Flow of FIPS 140-2 Testing and Validation
NVLAP Accredited FIPS 140-2 CMT Lab
Vendor selects a lab; Submits module for testing; Module IUT
Cryptographic Module Vendor
1
Test for conformance To FIPS 140-2; Writes test report
1a
Lab submits questions for guidance and clarification
NIST/CSE issue testing and Implementation Guidance
Issue validation certificate (via lab to the vendor)
5a
4
Module Coordination
Module's Test Report
Cost Recovery Fee Received Prior to Validation
2
CMT Test Report to NIST/CSE for validation; Module Review Pending
NIST/CSE
3
Reviewer Assigned Module Under Review
List of Validated FIPS 140-2 Modules
5
Finalization; NIST adds module to validated modules list at www.nist.gov/cmvp

Figure 1: General Flow of FIPS 140-2 Testing and Validation.

(Source: FAQs for the CMVP, NIST&CSE, May 20, 2005)

The CMVP can be applied to any government department, although it is only current formally accepted by the U.S., Canadian, and U.K. governments only for the time being. Currently, several Common Criteria (CC) Protection Profiles (PP) require FIPS 140-1 and 140-2 validated cryptographic modules. These PPs have been developed by many organizations throughout the world. Using FIPS 140-2 validated cryptographic modules will ensure that the product has implemented the FIPS approved/NIST recommended cryptography correctly (WEB_5 2006).

The role of the CMT Laboratories is to test the cryptographic module against all applicable requirements as specified in FIPS 140-2 and in the cryptographic algorithm standards and record the results. If a cryptographic module conforms to all the functional and assurance requirements as stated in the "**Derived Test Requirements (DTR)**", the CMT laboratory submits a written report to the Validation Authorities. If a cryptographic module does not meet one (or more) requirements, the CMT Laboratory will work with the vendor to resolve all discrepancies prior to resubmitting the validation package to the Validation Authorities (WEB_5 2006).

Typically, for cryptographic algorithms, the CMT laboratory generates test vectors based on information provided by the vendor. The CMT laboratory and the vendor use test vectors to exercise the cryptographic algorithm implementation. The vendor submits test results to the CMT laboratory and the laboratory verifies that the results are accurate (WEB_5 2006).

The testing process duration depends on the cryptographic module being tested. The time depends on a variety of factors including: the complexity of the cryptographic module, the overall Security Level, individual Security Levels (if higher than the overall Security Level), the current lab workload, and the content and quality of the vendor documentation submitted with the cryptographic module (WEB_5 2006).

To test cryptographic modules to FIPS 140-2, **"Security Requirements for Cryptographic Modules"**, and cryptographic algorithm standards, CMT laboratories become an accredited CMT laboratory under either National Validation Laboratory Accreditation Program (NVLAP) or Standards Council of Canada (SCC). All CMT laboratories are currently accredited by NVLAP. In Canada, SCC is preparing a CMT laboratory accreditation process under the Program for Accreditation of Laboratories – Canada (PALCAN). PALCAN will support the review of the Quality System with technical assistance from the CMVP staff (WEB_5 2006).

A cryptographic module does not meet the requirements or conform to the FIPS 140-1 or FIPS 140-2 standard unless a reference can be made to the validation certificate number obtained by CMVP. The module used must also be the same version/part number as annotated on the validation certificate. Any other claims are not relevant (WEB_5 2006).

3.3. Related Studies

Due to confidentiality of the topic, it is not easy to find/survey previous studies related to what is proposed in this study in Turkey. In the following paragraphs we shall mention about some related studies that have additional and beneficial information (beyond FIPS 140-2) for the set up of our template technical specification for the cryptographic modules, anyhow.

3.3.1. Case Study # 1

The study entitled **"Side-Channel Attacks:Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing"** by YongBin Zhou and DengGuo Feng, denotes that side-channel attacks are easy-to-implement whilst powerful attacks against cryptographic implementations, and their targets range from primitives, protocols, modules, and devices to even systems. These attacks pose a serious threat to the security of cryptographic modules. In consequence, cryptographic implementations have to be evaluated for their resistivity against such attacks and the incorporation of different countermeasures has to be considered. This study surveys the methods and techniques employed in these attacks, the destructive effects of such attacks, the countermeasures against such attacks and evaluation of their feasibility and applicability. Finally, the necessity and feasibility of adopting this kind of physical security testing and evaluation in the development of FIPS 140-3 standard are explored (WEB_6 2006).

Actually, there are some problems with the current version of FIPS 140-2. First of all, this version of standard is mainly focused on **"hardware modules"**, and is not well adapted to software modules. It is expected this status may change in the coming version of FIPS 140-3. Secondly, this version of standard covers somewhat too narrow scopes of the system to be tested. Better alignment with the **"Common Criteria"** is required, and the security vulnerabilities of functional protocols need to be addressed better. Finally, the functional requirements of this version of FIPS 140-2 are already out-of-date. The requirements specified in FIPS 140-2 have lagged behind the actual needs of the information security both in theory and practice (WEB_6 2006).

Meanwhile, the complex process of FIPS 140-2 validation shows that excellence in creating solid cryptographic algorithms and modules is difficult to achieve. Of the eleven areas, the following four areas are likely of greatest difficulty: **“physical security, self-tests, random number generation and key management”** (WEB_6 2006).

Specifically, as far as Side-Channel Attack (SCA) is concerned, FIPS 140-1 did not explicitly mention the security of cryptographic modules against side channel attacks, while FIPS 140-2 only deal briefly with the specification of mitigation of attacks for which no testable requirements are currently available. The most common and known SCAs with some details (WEB_6 2006) are:

- **Timing Attack:** Implementations of cryptographic algorithms often perform computations in non-constant time, due to performance optimizations. If such operations involve secret parameters, these timing variations can leak some information and, provided enough knowledge of the implementation is at hand, a careful statistical analysis could even lead to the total recovery of these secret parameters. A timing attack is, essentially, a way of obtaining some user's private information by carefully measuring the time it takes the user to carry out cryptographic operations. The principle of this attack is very simple: to exploit the timing variance in the operation. Two common countermeasures that are currently in use (i.e. noise injection and branch equalization) appear to be fundamentally different in the sense that noise injection weakens the power of the timing attack but it does not defeat it, whereas branch equalisation does defeat the attack but at significant cost.

- **Fault Attack:** Most of the devices that perform various cryptographic operations are usually assumed to operate reliably when we use them, so we might not think to question if the security of such operations depend on the reliability of these devices that implement them. In spite of this assumption, hardware faults and errors occurring during the operation of a cryptographic module in fact have been demonstrated to seriously affect the security. These faulty behaviors or outputs may also become important side channels, and will even greatly increase a cipher's vulnerability to cryptanalysis sometimes. Generally speaking, a successful fault attack on cryptographic modules or devices requires two steps: the fault injection and the fault exploitation steps. If we suppose that an attacker cannot induce the same fault twice, one of the best countermeasures to protect the symmetric algorithms such DES and AES is to compute the whole or a part of the rounds twice (including key scheduling). Another countermeasure suggested to protect public key algorithms from some specific fault attacks is to check the integrity of the secret key at the end of signature computation.

- **Power Analysis Attack:** In addition to its running time and its faulty behaviour, the power consumption of a cryptographic device may provide much information about the operations that take place and the involved parameters. This is the very idea of power analysis attack. Certainly, power analysis attack is applicable only to hardware implementation of the cryptosystems.

Power analysis attack is particularly effective and proven successful in attacking smart cards or other dedicated embedded systems storing the secret key. Basically, power analysis attack can be divided into Simple and Differential Power Analysis (referred to as SPA and DPA, respectively). In SPA attacks, the aim is essentially to guess from the power trace which particular instruction is being executed at a certain time and what values the input and output have. Therefore, the adversary needs an exact knowledge of the implementation to mount such an attack. On the other hand, DPA attack does not need the knowledge of the implementation details and alternatively exploiting statistical methods in the analysis process.

Proposals for hardware-based defenses against power analysis attacks include using an internal power source, randomizing the order in which instructions are executed, randomized register renaming, and using two capacitors, one of which is charged by an external power supply and the other supplies power to the device. One effective method for guarding against SPA attacks on point multiplication is to employ elliptic curve addition formulas that can also be used for doubling.

Defenses against differential power analysis are difficult, since they essentially only reduce the signal the adversary is reading, rather than eliminate it. Interestingly, an efficient randomization technique, using some random variables within the point addition operation, has also been proposed as a possible countermeasure against a DPA-style attack on the window-family algorithm in.

- **EM Attack:** As electrical devices, the components of a computer often generate electromagnetic radiation as part of their operation. An adversary that can observe these emanations and can understand their causal relationship to the underlying computation and data may be able to infer a surprising amount of information about this computation and data. This ability can be devastating, should the computer be a trusted computing platform intended to keep this information from the adversary. Similar to the power analysis attacks, ElectroMagnetic Analysis (EMA) attacks can also be divided into two main categories: Simple ElectroMagnetic Analysis (SEMA) and Differential ElectroMagnetic Analysis (DEMA). Countermeasures against EM attacks on specific implementations fall into two broad categories: ***signal strength reduction*** and ***signal information reduction***. Techniques for signal strength reduction include circuit redesign to reduce unintentional emanations and the use of shielding and physically secured zones to reduce the strength of compromising signals available to an adversary relative to ambient thermal noise. Techniques for signal information reduction rely on the use of randomization and/or frequent key refreshing within the computation so as to substantially reduce the effectiveness of statistical attacks using the available signals.

- **Acoustic Attack :** Most side-channel attack research has focused on electromagnetic emanations (TEMPEST), power consumption and, recently, diffuse visible light from CRT displays. However, one of the oldest eavesdropping channels, namely acoustic emanations, has received little attention. Very recently, Shamir have demonstrated a preliminary proof-of-concept that a correlation exists between the sound of a processor and its computation. One may consider the approach the P. Wright used in 1965 is likely one of the primitive acoustic attacks. However, this is a relatively new field, and much work needs to be done.

- **Visible Light Attack :** Kuhn demonstrated (via both sophisticated analysis as well as direct experiment) that the average luminosity of a CRT's diffuse reflection off of a wall can sufficient to reconstruct the signal displayed on the CRT (so shielding the CRT to protect against leaking information via electromagnetic radiation may not be sufficient). One outstanding characteristic of this attack is that physical access is not required.

- **Error Message Attack :** In many standards, e.g. SSL/TLS, IPSEC, WTLS, messages are first pre-formatted, then encrypted in CBC mode with a block cipher. Decryption needs to check if the format is valid. Validity of the format is easily leaked from communication protocols in a chosen ciphertext attack since the receiver usually sends an acknowledgment or an error message. This can become a useful side channel for cryptanalysis and the attack exploiting this side channel is often called error message attack.

- **Cache-based Attack :** Previously proposed timing attacks make use of the fact that conditional branches that occur during encryption processing cause variations in encryption time. CPU cache misses, however, can also cause such variations. In this regard, most of the recent computers employ a **CPU cache**, abbreviated simple to a **cache** from here on, between the CPU and main memory, since this type of hierarchical structure can speed program run-time on the average. If, however, the CPU accesses data that were not stored in the cache, i.e. if a cache miss occurs, a delay will be generated, as the target data must be loaded from main memory into the cache. The measurement of this delay may enable attackers to determine the occurrence and frequency of cache misses. This is where the cache-based side channel attacks goes. A number of countermeasures to mitigate the cached-based attacks have been proposed, to name a few, to remove cache or cached S-box access, to disable cache flushing, to perform time and miss skewings, to use application-specific algorithmic masking, to depend on operating system support, to adopt partitioned cache hardware architecture, and so on.

- **Frequency-based Attack :** C.C. Liu proposed a frequency-based side channel attack against mobile devices such as PDAs, cell phones and pagers. His method is efficient even when traces are misaligned in actual attacking experiments, whereas the previously researched DEMA fails in such condition. In addition, the proposed first-order frequency attack is capable of defeating the desynchronization countermeasure that randomly inserts delays. However, it may be a pity that the countermeasures against this kind of frequency-based attack are not addressed.

- **Scan-based Attack :** Scan based test is a powerful test technique. However, it is an equally powerful attack tool. In 2004, Yang used scan chains as a side channel to recover secret keys from a hardware implementation of DES. By using one build-in self-test scheme, the internal status of cryptographic chips will not be scanned out and such scan based attacks can be avoided. Luckily enough, this kind of self-test is already recommended by FIPS 140-2 be the physical security requirement of cryptographic chips. However, it is pointed out here that the high fault coverage of scan based test makes developing a secure scan based solution to cryptographic chips interesting.

Besides the current security testing requirements, the requirements of standard FIPS 140-2 should be extended to a larger scale and to cover the following aspects like side channels mentioned above: **“analysis of cryptographic protocols”**; **“analysis of effectiveness of key management”**; **“analysis of correct use of the cryptographic module in a larger product”**; **“any statements about non-FIPS approved or FIPS allowed algorithms”**; and so on (WEB_6 2006). The topics on “analysis of correct use of the cryptographic module in a larger product” and “any statements about non-FIPS approved or FIPS allowed algorithms” are out of concern in this study, but, it is thought that is essential to explain “analysis of cryptographic protocols” and “analysis of effectiveness of key management” aspects briefly in the following paragraphs due to the importance for the study.

3.3.1.1.Analysis of Cryptographic Protocols

Analyzing the cryptographic protocols needs to test “secrecy” (the adversary cannot obtain the secret), “authentication” and “strong secrecy” (the adversary does not see the difference when the value of the secret changes) features of the cryptographic protocol. And the most common and effective methods for analyzing and documenting the cryptographic protocol operations, according to their operation domain, are (Gritzalis and Spinellis 1997): “**Inference-construction”**, “**Attack-construction”** and **“Proof-construction”**.

- **Inference-construction:** Inference analysis is a class of analyses that builds a framework of modal logic around properties such as knowledge and beliefs of the participants in a protocol. The first logic system for protocol analysis was the so-called BAN logic devised by Burrows, Abadi and Needham . It assumes that authentication is a function of integrity and freshness, and uses logical rules to trace both of those attributes through the protocol. There are three main stages for the analysis of a protocol using BAN logic. The first step is to express the assumptions and goals as statements in a symbolic notation so that the logic can proceed from a known state to one where it can ascertain whether the goals are in fact reached. The second step is to transform the protocol steps into symbolic notation. Finally, a set of deduction rules called postulates are applied. The postulates should lead from the assumptions, via intermediate formulas, to the authentication goals. The BAN logic has been extended in, amongst others, GNY and SvO. Inference analysis of cryptographic protocol has shown to be a success (Lukell and Hutchison 2003).

- **Attack-construction:** As the name indicates, this kind of methods construct probable attack sets based on the algebraic properties of the protocol's algorithms. Examples of such methods are the NRL Protocol Analyzer, and Lowe's method of using the FDR model checker. These methods are targeted towards ensuring authentication, correctness or secrecy properties of the analysed protocols. Their disadvantage lies in the big number of possible events that must be examined, also referred to the *state space explosion problem*. However, various optimisation techniques exist that limit the search space to a manageable size. Furthermore, in combination with the development of more powerful computer systems, this approach has shown to be viable for modelled systems of a reasonable size (Lukell and Hutchison 2003).

- **Proof Construction:** Attempts to avoid the exponential searches of attack construction, and to extend analyses that involve arbitrarily large numbers of participants and messages, has given rise to the proof construction approach for the analysis of protocol failures. It has the potential of being as thorough as attack construction in proving possible attacks, while avoiding exponential searches by replacing them with theorems about these searches. This method is completely general, with the disadvantage that it typically requires significant human insight and guidance (Lukell and Hutchison 2003).

3.3.1.2.Analysis of Effectiveness of Key Management

Key management is often an afterthought in the cryptographic development process. As a result, cryptographic subsystems too often fail to support the key management functionality and protocols that are necessary to provide adequate security with the minimum necessary reduction in operational efficiency. But, there is no testing method avaliable for "Key Management" currently, since FIPS 171 "Key Management Using ANSI X9.17" is withdrawn by NIST on February 8, 2005 due to withdrawal of X9.17 by ANSI. But **"Recommendation for Key Management Guideline- Part 1:General"** has been approved by NIST as "NIST Special Publication 800-57" in August 2005. This first part is quite informative and provides initiative for the rest of the "Key Management".To summarize the Part 1:General (NIST 2005):

- All cryptographic development activities **should** involve key management planning and specification by those managers responsible for the secure implementation of cryptography into an information system.

- Key management planning **should** begin during the initial conceptual/development stages of the cryptographic development lifecycle, or during the initial discussion stages for the application of existing cryptographic components into information systems and networks.

- For cryptographic development efforts, a key specification and acquisition planning process **should** begin as soon as the candidate algorithm(s) and, if appropriate, keying material medium and format have been identified.

- For the application of existing cryptographic products for which no key management specification exists, the planning and specification processes **should** begin during device and source selection and continue through acquisition and installation.

- **Key Management Specification Description/Purpose :** The Key Management Specification is the document that describes the key management components that may be required to operate a cryptographic device throughout its lifetime.

- **Content of the Key Management Specification :** The Key Management Specification **should** contain a title page that includes the device identifier, and the developer's or integrator's identifier. A revision page, list of reference documents, table of contents, and definition of abbreviations and acronyms page **should** also normally be included.

- **Cryptographic Application :** The Cryptographic Application section provides a brief description of the cryptographic application or proposed employment of the cryptographic device. This includes the purpose or use of the cryptographic device (or application of a cryptographic device), and whether it is a new cryptographic device, a modification of an existing cryptographic device, or an existing cryptographic device for which a Key Management Specification does not exist. A brief description of the security services (confidentiality, integrity, non-repudiation, access control, identification and authentication, and availability) that the cryptographic device/application provides **should** be included. Information concerning longterm and potential interim key management support (key management components) for the cryptographic application **should** be provided.

- **Communications Environment :** The Communications Environment section provides a brief description of the communications environment (like data networks (intranet, internet, VPN)) in which the cryptographic device is designed to operate.

- **Key Management Component Requirements :** The key management component requirements section describes the types and logical structure of keying material required for operation of the cryptographic device. Cryptographic applications using public key certificates (i.e., X.509

certificates) **should** describe the types of certificates supported. The following information **should** be included:

- The different keying material classes or types required, supported, and/or generated (e.g., for PKI: CA, signature, key establishment, and authentication).

- The key management algorithm(s) (the applicable FIPS).

- The keying material format(s) (reference any existing key specification if known).

- The set of acceptable PKI policies (as applicable).

- Tokens to be used.

- **Key Management Component Generation :** This section of the Key Management Specification **should** describe requirements for the generation of key management components by the cryptographic device for which the Key Management Specification is written.

- **Key Management Component Distribution :** Where a device supports the automated distribution of keying material, this section of the Key Management Specification **should** describe the distribution and transport encapsulation (where employed) of keying material supported by the device.

- **Keying Material Storage :** This section of the Key Management Specification **should** address how the cryptographic device or application for which the Key Management Specification is being written stores information, and how the keying material is identified during its storage life (e.g., Distinguished Name). The storage capacity capabilities for information **should** be included.

- **Access Control :** This section of the Key Management Specification **should** address how access to the cryptographic device components and functions is to be authorized, controlled, and validated to request, generate, handle, distribute, store, and/or use keying material. Any use of passwords and personal identification numbers (PINs) **should** be included. For PKI cryptographic applications, role-based privileging and the use of tokens **should** be described.

- **Accounting :** This section of the Key Management Specification **should** describe any device or application support for accounting for keying material. Any support for or outputs to logs used to support the tracking of key management component generation, distribution, storage, use and/or destruction **should** be detailed. The use of appropriate privileging to support the control of keying material that is used by the cryptographic application **should** also be described, in addition to the directory capabilities used to support PKI cryptographic applications, if applicable. The Key Management Specification **shall** identify where human and automated tracking actions are required and where two-person integrity is required, if applicable.

- **Compromise Management and Recovery :** This section of the Key Management Specification **should** address any support for the restoration of protected communications in the event of the compromise of keying material used by the cryptographic device/application. The recovery process description **should** include the methods for re-keying.

- **Key Recovery :** This section of the Key Management Specification describes product support or system mechanisms for effecting key recovery. Key recovery addresses how unavailable encryption keys can be recovered. System developers **should** include a discussion of the generation, storage, and access for long-term storage keys in the key recovery process description. The process of transitioning from the current to future long-term storage keys **should** also be included.

3.3.2. Case Study # 2

The study entitled **"Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems"** by Gonzalo Alvarez and Shujun Li, denotes that many proposed systems are difficult to implement in practice with a reasonable degree of security. Likewise, they are seldom accompanied by a thorough security analysis. Consequently, it is difficult for other researchers and end users to evaluate their security and performance. In this study it is intended to provide a common framework of basic guidelines that, if followed, every new cryptosystem would benefit from. The suggested guidelines address three main issues: implementation, key management, and security analysis, aiming at assisting designers of new cryptosystems to present their work in a more systematic and rigorous way to fulfill some basic cryptographic requirements (Alvarez and Li 2006).

3.3.3. Case Study # 3

The study entitled **"Cryptographic Processors-A Survey"** by Ross Anderson, Mike Bond, Jolyon Clulow and Sergei Skorobogatov, denotes that one response is to look for evaluations by third parties. There are two schemes under which cryptoprocessors are certified FIPS 140, run by the US National Institute of Standards and Technology, and the Common Criteria, operated by a number of member countries. Both have drawbacks. FIPS looks only at the tamperresistance of the hardware. A FIPS evaluation, especially at level 4, is nonetheless of value to the discerning customer (Anderson et al. 2006).

3.3.4. Case Study # 4

The study entitled **"An Open-source Cryptographic Coprocessor"** by Peter Gutmann explains that current crypto implementations rely on software running under general-purpose operating systems alongside a horde of untrusted applications, ActiveX controls, web browser plugins, mailers handling messages with embedded active content, and numerous other threats to security, with only the OS's (often almost nonexistant) security to keep the two apart. The study also presents a general-purpose open-source crypto coprocessor capable of securely performing crypto operations such as key management, certificate creation and handling, and e-mail encryption, decryption, and signing, at a cost one to two orders of magnitude below that of commercial equivalents while providing generally equivalent performance and a higher level of functionality. The study examines various issues involved in designing the coprocessor, and explores options for hardware acceleration of crypto operations for extended performance above and beyond that offered by the basic coprocessor's COTS hardware (Gutmann 2000).

3.3.5. Case Study # 5

The study entitled **"The Design and Verification of a Cryptographic Security Architecture"** by Peter Gutmann again, denotes, in **Chapter 2 Security Architecture,** when building a secure system for cryptographic use, there are two possible approaches which can be taken. The first is to build (or buy) a general-purpose kernel-based secure operating system and run the crypto code on top of it, and the second is to build a special-purpose kernel which is designed to provide security features which are appropriate specifically for cryptographic applications. Building the crypto code on top of an existing system is explicitly addressed by FIPS 140, the one standard which specifically targets crypto modules. This requires that, where the crypto module is run on top of an operating system which is used to isolate the crypto code from other code, it be evaluated at progressively higher Orange Book levels for each FIPS 140 level, so that security level 2 would require the software module to be implemented on a C2-rated operating system. This provides something if an impedance mismatch between the actual security of equivalent hardware and software crypto module implementations, it's possible that the these security levels were set so low out of concern that setting them any higher would make it impossible to implement the higher FIPS 140 levels in software due to a lack of systems evaluated at that level. For example trying to source a B2 or more realistically B3 system to provide an adequate level of security for the crypto software is almost impossible (the practicality of employing an OS in this class, whose members include Trusted Xenix, XTS 300, and Multos, speaks for itself) (Gutmann 2003).

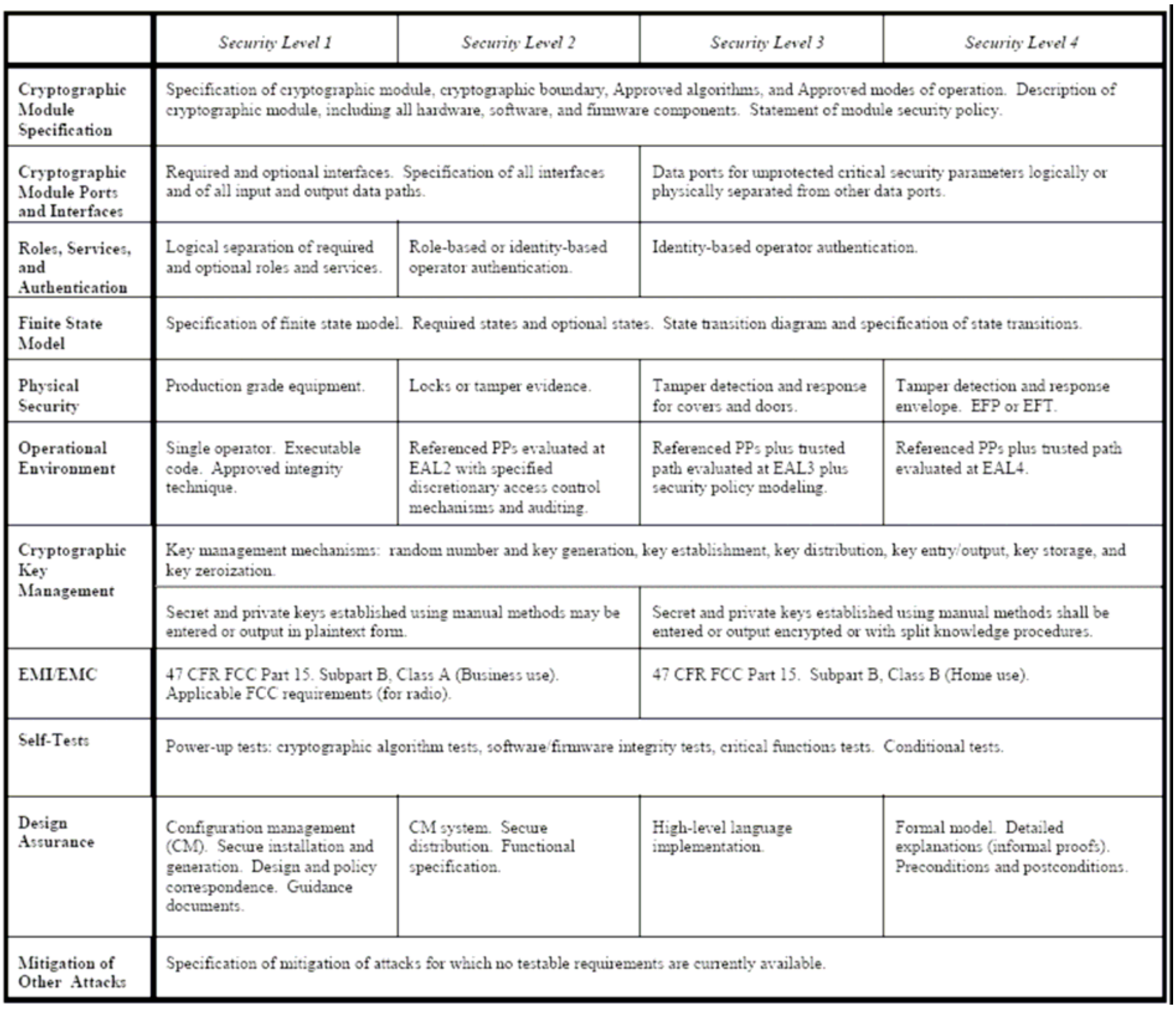
Another work which examines crypto software modules also recognises the need to protect the software through some form of security kernel based mechanism, but views implementation in terms of a device driver protected by an existing operating system kernel. The suggested approach is to modify an existing kernel to provide cryptographic support (Gutmann 2003).

Two decades of experience in building high-assurance secure systems have shown that an approach which is based on the use of an application-specific rather than general-purpose kernel is the preferred one. For example in one survey of secure systems carried out during the initial burst of enthusiasm for the technology, most of the projects discussed were special-purpose filter or guard systems, and for the remaining general-purpose systems a recurring comment is of poor performance, occasional security problems, and frequent mentions of verification being left incomplete because it was too difficult. Although some implementors did struggle with the problem of kernel size and try to keep things as simple as possible, attempts to build general-purpose secure OS kernels appear to have foundered, leaving application-specific and special-purpose kernels as the best prospect for successful implementation (Gutmann 2003).

3.4. Comparison of FIPS 140-2 with Technical Specifications.

As mentioned before, security requirements that shall be satisfied by cryptographic modules conforming to FIPS 140-2, cover areas related to the design and implementation of a cryptographic module and they also cover the areas of cryptographic module specification; module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; and of design assurance. An additional area concerned with the mitigation of other attacks is currently not tested but the vendor is required to document the implemented controls (e.g., differential power analysis, and TEMPEST). Table 1 summarizes the security requirements in each of these areas (WEB_2 2006)

Table 1: FIPS 140-2 Security Requirements in Each Security Level.
(Source: FIPS PUB 140-2 Security Requirements For Cryptographic Modules)



	Security Level 1	*Security Level 2*	*Security Level 3*	*Security Level 4*
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.			
Cryptographic Module Ports and Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters logically or physically separated from other data ports.	
Roles, Services, and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Finite State Model	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. EFP or EFT.
Operational Environment	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.
Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.			
	Secret and private keys established using manual methods may be entered or output in plaintext form.		Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.	
EMI/EMC	47 CFR FCC Part 15. Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15. Subpart B, Class B (Home use).	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.			
Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	CM system. Secure distribution. Functional specification.	High-level language implementation.	Formal model. Detailed explanations (informal proofs). Preconditions and postconditions.
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available.			

A cryptographic module shall be tested against the requirements of each area addressed in Table 1. The cryptographic module shall be independently rated in each area. Several areas provide for increasing levels of security with cumulative security requirements for each security level. In these areas, the cryptographic module will receive a rating that reflects the maximum security level for which the module fulfills all of the requirements of that area. In areas that do not provide for different levels of security (i.e., standard set of requirements), the cryptographic module will receive a rating commensurate with the overall level of security (WEB_2 2006).

In addition to receiving independent ratings for each of the security areas, a cryptographic module will also receive an overall rating. The overall rating will indicate the minimum of the independent ratings received in the areas.

As any one can easily guess, this study is a comparative one, between FIPS 140-2 and the formerly (before FIPS 140-2) used technical specifications for governmental cryptographic module procurements. The best way to compare is thought as to analyze all the specifications item by item and try to determine the similarities and/or differences with the ones in FIPS 140-2 above mentioned 11 areas in a table format.

3.4.1. Construction of Comparison Table

The next job after general explanation of the standard and technical specifications, is to form a “Comparison Table”, which compares FIPS 140-2 requirements with the technical specifications formerly used for governmental procurements. Three different specifications were surveyed and analyzed item by item. The cells which left blank and shaded with gray in the comparison table designate that no corresponding item(s) were found in that specific technical specification for procurement. Since the comparison table; being as it is, is somewhat lengthy, included in APPENDIX A which is in CD that comes with this thesis.

3.4.2. Evaluation of Comparison Table

To evaluate the Comparison Table we need to compare each technical specification items with the ones FIPS has. Even though it is not possible to find one to one similarity between the items of the specifications and the items in FIPS 140-2, we accepted the **“likelihood”** as sufficient for correspondance.

3.4.2.1. Evaluation of Technical Specification # 1

After analyzing the Technical Specification # 1, we can observe that the following FIPS items have no counterpart in Technical Specification # 1, possibly depending on the needs:

- 4.3.2 Services.
- 4.4 Finite State Model.
- 4.5.2 Physical Security Requirements for Single-Chip Cryptographic Modules.
- 4.5.3 Physical Security Requirements for Multiple-Chip Embedded Cryptographic Modules.
- 4.5.4 Physical Security Requirements for Multiple-Chip Standalone Cryptographic Modules.
- 4.6 Operational Environment.
- 4.6.1 Operating System Requirements.
- 4.7.1 Cryptographic Key Mgmt. Random Number Generators (RNG).
- 4.7.2 Cryptographic Key Mgmt. Key Generation.
- 4.7.3 Cryptographic Key Mgmt. Key Establishment.
- 4.9.2 Self Tests Conditional Tests.
- 4.10.1 Design Assurance Configuration Mgmt.
- 4.10.2 Design Assurance Delivery and Operation.
- 4.10.3 Design Assurance Development.

- 4.10.4 Design Assurance Guidance Documents.

And the non-satisfying parts (wrt. security levels) of partially covered items are:

- 4.2 Cryptographic Module Ports and Interfaces (Security Level 3,4).
- 4.3.3 Authentication (Security Level 1,3,4).
- 4.5.1 General Physical Security Requirements (Security Level 2,3,4).
- 4.5.5.1 Environmental Failure Protection Features (Security Level 1).
- 4.5.5.2 Environmental Failure Testing Procedures (Security Level 1).
- 4.7.4 Cryptographic Key Mgmt. Key Entry and Output (Security Level 3,4).
- 4.8 Electromagnetic Interference (EMI), Electromagnetic Compatibility (EMC) (Security Level 3,4).

Besides all, it is evaluated that the explanations related to the cyrptographic module are insufficient in Technical Specification # 1.

3.4.2.2. Evaluation of Technical Specification # 2

The Technical Specification # 2 is very similar, if not identical, to the Technical Specification # 1 from the missing items point of view. However, it does manage to have the below listed items which have their counterparts in FIPS 140-2.

- 4.3.3 Authentication (Security Level 1).
- 4.5.1 General Physical Security Requirements (Security Level 3).
- 4.9.2 Self Tests Conditional Tests.

3.4.2.3. Evaluation of Technical Specification # 3

The almost identical evaluations with Technical Specification # 1 can be done for Technical Specification # 3, too. But Technical Specification # 3 also has items corresponding following FIPS 140-2 items, as different from Technical Specification # 1:

- 4.5.1 General Physical Security Requirements (Security Level 3).
- 4.7.1 Cryptographic Key Mgmt.(Security Level 1).

And the following FIPS 140-2 items have never been mentioned as different from Technical Specification#1:

- 4.3.1 Roles.
- 4.3.2 Services.
- 4.3.3 Authentication.

CHAPTER 4

CONCLUSIONS

4.1. Evaluations

On the way for **“Defining A Sample Template For Governmental Procurements of Cryptographic Products”**, surveying the FIPS 140-2 itself, the studies related with the FIPS 140-2 (or concerning FIPS 140-2) and the comparing FIPS 140-2 with Technical Specifications formerly used for procurement of cryptographic modules, shall result with the following evaluations of FIPS 140-2 as the main concentration and the basis of this study.

4.1.1. The Strengths

- FIPS 140-2 (with whole text containing punctuation) has been accepted as “**ISO/IEC 19790:2006”** and this tells us that similar official standardization work will be initiated in Turkey in near future. This also shall lead the establishment of additional “Validation Labs” worldwide, possibly in Turkey, too.

- FIPS 140-2 (or ISO/IEC 19790:2006) has explicit superiority in defining a cryptographic module over the technical specifications formerly used. In the specification of cryptographic modules “Services, Finite State Model, Physical Security Requirements, Operational Environment, Cryptographic

Key Management, Self Tests (Conditional Tests) and Design Assurance" sections have no counterpart in the analyzed specifications and they are where the FIPS 140-2 obtains its superiority.

- Scan based test is a powerful test technique and scan chains can also be used as a side channel attack to recover secret keys from a hardware implementation of DES. By using one build-in self-test scheme, the internal status of cryptographic chips will not be scanned out and such scan based attacks can be avoided. Luckily enough, this kind of self-test is already recommended by FIPS 140-2 be the physical security requirement of cryptographic chips (WEB_6 2006).

- However, there is not any single item which refers to this in either of the surveyed technical specifications in this study.

4.1.2. The Weaknesses

- FIPS 140-2 is mainly focused on **"hardware modules"**, and is not well adapted to software modules (WEB_6 2006) FIPS 140-2 demonstrates obvious evidences for this assessment in section "4.5. Physical Security Requirements".

- FIPS 140-2 covers somewhat too narrow scopes of the system to be tested. Better alignment with the **"Common Criteria"** is required, and the security vulnerabilities of functional protocols need to be addressed better (WEB_6 2006).

- If you need the flexibility of having FIPS 140-2 Validation for multiple operating system platforms, the ideal security level is FIPS 140-2 Security

Level 1. At FIPS 140-2 Security Level 2, you become restricted to the platforms that are approved according to Common Criteria (WEB_2 2006).

- FIPS 140-2 Validation is platform specific: individual validation certificate numbers are required for each platform. Moreover, any changes or additions to a validated product require revalidation, incurring additional costs (WEB_2 2006).

- The complex process of FIPS 140-2 validation shows that excellence in creating solid cryptographic algorithms and modules is difficult to achieve. Of the eleven areas, the following four areas are likely of greatest difficulty: **"physical security, self-tests, random number generation and key management"** (WEB_6 2006).

- Specifically, as far as **"side channel attacks"** are concerned, FIPS 140-1 did not explicitly mention the security of cryptographic modules against side channel attacks, while FIPS 140-2 only deal briefly with the specification of mitigation of attacks for which no testable requirements are currently available (WEB_6 2006). In Section **"4.11. Mitigation of Other Attacks"** a few well-known SCA is concerned and they are: "Power Analysis", "Timing Analysis", "Fault Induction" and "TEMPEST". Nevertheless the following common and known SCAs which have no place in FIPS 140-2 should have been discussed and evaluated in paragraphs of the future FIPS documentation: "EM Attack", "Acoustic Attack", "Visible Light Attack", "Error Message Attack", "Cache-based Attack", "Frequency Based Attack", "Scan-based Attack".

4.2. Results

In the light of the above evaluations, “to define a sample template for governmental procurements of cryptographic products” the following results are derived:

- The present context of FIPS 140-2 which is mainly focusing on “hardware modules” is thought to be acceptable and sufficient for the aim of this study, since the demand for software cryptographic modules is none or negligible comparing with the demands for hardware/firmware modules of governmental organizations.

- Even though it is evaluated and claimed in a study that, better alignment with the **“Common Criteria”** is required (WEB_6 2006) , in section **“4.6.1. Operating System Requirements”** of FIPS 140-2, target operating system is required to meet the conditions of Common Criteria **“EAL2 to EAL4”** respectively for **“Security Levels 2 to 4”.** And any further interaction with Common Criteria components, but the ones with operating systems, seems unnecessary due to almost perfect inclusion of FIPS 140-2 on other topics.

- The requirements of standard FIPS 140-2 should be extended to a larger scale and to cover the following aspects: **“analysis of cryptographic protocols”**; **“analysis of effectiveness of key management”**; **“analysis of side channels or similar vulnerabilities”** (WEB_6 2006).

4.3. Recommendations

Ultimately, FIPS 140-2 (or ISO/IEC 19790:2006) is recommended and thought to be used as the basis document to prepare a sample template specification. To form the facilitating template due to demands of the governmental organization, **"Sample Template Specification for Cryptographic Modules"** and facilitative **"Sample Template Specification Matrix for Cryptographic Modules"** have been prepared (in Turkish) under the guidance of above evaluations & related results and by depending on **"M.S.B. Teknik Şartname Hizmetleri Yönergesi** (**MSY.: 202-12 (B))"** and placed in **APPENDIX B** and **APPENDIX C** to this study, respectively.

The lack of any paragraph related to **"Analysis of Cryptographic Protocols"** in FIPS 140-2 has no sense and may result with deficiency in "Validation of Cryptographic Modules". To overcome this probable problem, the sub-topic of **"Analysis of Cryptographic Protocols"** is recommended to place and placed as a paragraph in section **"2.12. Analysis of Cryptographic Protocol"** of proposed Sample Template Specification.

Due to insufficiency of **"FIPS 140-2 Section 4.11. Mitigation of Other Attacks"** for providing solutions to most of SCAs, but only Power Analysis, Timing Analysis, Fault Induction and TEMPEST, the rest of the well-known SCAs and the known counter-measures for each attack are recommended to place and placed in the section **"2.11. Mitigation of Other Attacks"** of proposed Sample Template Specification.

Since **"Key Management"** is often an afterthought in the cryptographic development process and this result cryptographic subsystems too often to fail to support the key management functionality and protocols, it is a must to test Key Management before going any further for validation of any cryptographic module. But, there is no testing method avaliable for "Key Management" currently, since FIPS 171 "Key Management Using ANSI X9.17" is withdrawn by NIST on February 8, 2005 due to withdrawal of X9.17 by ANSI. But again **"Recommendation for Key Management**

Guideline- Part 1:General” has been approved by NIST as **“NIST Special Publication 800-57”** in August 2005 and this might be accepted as one in the hand and better than nothing. Besides that, this first part is thought to be quite informative and providing initiative for the rest of the Key Management concerns. So the items forcing to prepare “Key Management Specification for Cryptographic Modules” are recommended to place and placed in the section **“Key Management”** of only APPENDIX (Documentation Requirements) of APPENDIX B.

The word by word translation of **“FIPS 140-2: Security Requirements for Cryptographic Modules”** into Turkish is prepared to facilitate to construct the Sample Template Specification and also to be research source in Turkish for future studies about this topic. FIPS 140-2 original and the Turkish translation of the FIPS 140-2 are placed in **APPENDIX D** to this study.

The Sample Template Specification Matrix in **APPENDIX C** might seem to be complex at first. That’s why it is also recommended to use **APPENDIX E “Web Based User Interface”** which is facilitating to simply construct a specification template in accordance with the governmental organization demands.

4.4. Future Work

Due to insufficiency of time and capability some works are left undone for the future studies. It is evaluated that the following future studies will provide additional and useful knowledge-base on this topic:

- Translation of “**Derived Test Requirements [DTR] for FIPS PUB 140-2”** into Turkish.
- Construction of **“Derived Test Requirements”** (in Turkish) as an annex to Sample Template Specification.
- Implementation of more intelligent and facilitative **“Specification Construction Software”** for governmental organizations.

REFERENCES

Alvarez G., Li S., 2006. “Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems”, International Journal of Bifurcation and Chaos, Vol.16, No.7.

Anderson R., Bond M., Clulow J., Skorobogatov S., 2006. “Cryptographic Processors-A Survey”, IEEE Proceedings, Vol.94, Issue.2, pp.357-369.

Başbakanlık, 2000. “Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı Taslağı”.

Gritzalis S., Spinellis D., 1997. “Cryptographic Protocols over Open Distributed Systems:A Taxonomy of Flaws and related Protocol Analysis Tools”, 16th International Conference on Computer Safety, Reliability and Security: SAFECOMP '97, pp.123-137.

Gutmann P., 2000. “An Open-source Cryptographic Coprocessor”, In Proceedings of 9th Usenix Security Symposium, Denver, Colorado (August 2000), pp.97-112.

Gutmann P., 2003. “The Design and Verification of a Cryptographic Security Architecture”, (Springer, New York), pp.43-44.

Lukell S., Hutchison A., 2003. “Attack Analysis of Cryptographic Protocols Using Strand Spaces”, South African Computer Journal, Issue.31, pp.25-32.

Milli Savunma Bakanlığı, 2003. “Savunma Sanayi Güvenliği Yönergesi”.

Milli Savunma Bakanlığı, 2006. “Araştırma Geliştirme ve Teknoloji Faaliyetleri Yönergesi MSY.: 380-1 (B)”.

Milli Savunma Bakanlığı, 2006. “ARGE ve Teknoloji Dairesi Başkanlığı ARGE Faaliyetleri Rehberi”.

NIST, 2005. "Special Publication 800-57: Recommendation for Key Management Guideline- Part 1:General".

WEB_1, 2006. "A Survey of Cryptography Laws and Regulations", 05/01/2006. http://rechten.uvt.nl/koops/THESIS/cryptocontroversy-ch05.PDF

WEB_2, 2006. FIPS PUB 140-2 Security Requirements For Cryptographic Modules, 05/01/2006. http://csrc.nist.gov/cryptval/

WEB_3, 2006. TÜBİTAK UEKAE (Kriptografik Test ve Tasarım), 26/05/2006. http://www.uekae.tubitak.gov.tr/faaliyet.htm

WEB_4, 2006. The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, 30/06/2006. http://www.wassenaar.org/controllists/index.html

WEB_5, 2006. "Frequently Asked Questions for the Cryptographic Module Validation Program", 26/05/2006. http://csrc.nist.gov/cryptval/140-1/CMVPFAQ.pdf

WEB_6, 2006. "Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing" (Cryptology ePrint Archive Web Site, Report 2005/388), 05/01/2006. http://eprint.iacr.org/