

**Guidelines for Preparing
Cryptographic Techniques
Application Documents**
(Provisional Translation)

June, 2000

Information-technology Promotion Agency, JAPAN
IT Security Center

Guidelines for Preparing Cryptographic Techniques Application Documents

For details on how to prepare the Cryptographic Techniques Application documents, see "4.2 Submission of Information Needed for Evaluation" in the Cryptographic Techniques Application Guidelines.

All printed documents must be in A4 format.

All electronic data must be in Microsoft WORD, Adobe PDF file or PostScript file formats. Use the following file names.

Store all electronic data together in an electronic medium (CD-R, CD-RW, or magneto-optical disk) and attach a label indicating the name of Cryptographic Techniques and the submitter's name.

- (1) Cryptographic Techniques Application Form(use the format on the attached sheet)
(Japanese or English)"call-1"
- (2) Cryptographic Techniques Overview(use the format on the attached sheet)
(Japanese)"call-2"
(English)"call-2e"
- (3) Cryptographic Techniques Specifications
(Japanese)"call-3"
(English)"call-3e"
- (4) Self Evaluation Reports
(Japanese)"call-4"
(English)"call-4e"
- (5) Test vector "call-5"
- (6) Sample code "call-6"
- (7) Information regarding the public availability status of the "specifications"
(Japanese) "call-7"
- (8) Information regarding intellectual property rights
(Japanese) "call-8"
- (9) Company Profile(use the format on the attached sheet)
(Japanese or English) "call-9"

Receipt Number	
-------------------	--

Application Date / /2000

TO Information-technology Promotion Agency, JAPAN

Applicant Name _____

(signature) _____

Cryptographic Techniques Application Form

Name of Cryptographic Technique	
Categories	1.Asymmetric Cryptographic Schemes 2.Symmetric Ciphers 3.Hush Functions 4.Pseudo-random Number Generators
Organization (company) name	
Submitter's name	
Submitter's Department and title	
Address (Postal Code)	
Phone number	
FAX number	
e-mail address web address	
Developer's name	
Developer's organization (company) name	

Information for each entry item is restricted to the designated pages. However, the applicant may decide how much page space to assign for any individual entry item.

Receipt Number	
-------------------	--

Cryptographic Techniques Overview

1. Name of Cryptographic Technique		
<table style="width: 100%; border: none;"> <tr> <td style="width: 15%; padding-right: 10px;">Categories</td> <td> <ul style="list-style-type: none"> 1.Asymmetric Cryptographic Schemes 2.Symmetric Ciphers 3.Hush Functions 4.Pseudo-random Number Generators </td> </tr> </table>	Categories	<ul style="list-style-type: none"> 1.Asymmetric Cryptographic Schemes 2.Symmetric Ciphers 3.Hush Functions 4.Pseudo-random Number Generators
Categories	<ul style="list-style-type: none"> 1.Asymmetric Cryptographic Schemes 2.Symmetric Ciphers 3.Hush Functions 4.Pseudo-random Number Generators 	
<table style="width: 100%; border: none;"> <tr> <td style="width: 15%; padding-right: 10px;">Security Functions of Asymmetric Cryptographic Schemes</td> <td> <ul style="list-style-type: none"> 1.confidentiality 2. Authentication 3. signature 4. key- sharing </td> </tr> </table>	Security Functions of Asymmetric Cryptographic Schemes	<ul style="list-style-type: none"> 1.confidentiality 2. Authentication 3. signature 4. key- sharing
Security Functions of Asymmetric Cryptographic Schemes	<ul style="list-style-type: none"> 1.confidentiality 2. Authentication 3. signature 4. key- sharing 	
<table style="width: 100%; border: none;"> <tr> <td style="width: 15%; padding-right: 10px;">Subcategories of Symmetric Ciphers</td> <td> <ul style="list-style-type: none"> 1. stream ciphers 2. 64-bits block ciphers 3. 128-bits block ciphers </td> </tr> </table>	Subcategories of Symmetric Ciphers	<ul style="list-style-type: none"> 1. stream ciphers 2. 64-bits block ciphers 3. 128-bits block ciphers
Subcategories of Symmetric Ciphers	<ul style="list-style-type: none"> 1. stream ciphers 2. 64-bits block ciphers 3. 128-bits block ciphers 	
2. Cryptographic Techniques Overview		
2.1 Design policy		
2.2 Intended applications		

Information for each entry item is restricted to the designated pages. However, the applicant may decide how much page space to assign for any individual entry item.

Receipt Number	
----------------	--

2.3 Basic theory and techniques

References of submission

Previous use

Company Profile

Company Name			
(President)	()		
Location(City)		Associated Companies	
Foundation Date			
Capital			
Number of Employees		Number of Engineers	
Major Organizations in which the company holds membership			
Key Operation of the Company			
Major Stockholder Names		Share Holdings(%)	
		(%)	