

# ISO/IEC TR 14516:2002-06 (E)

## Information technology - Security techniques - Guidelines for the use and management of Trusted Third Party services

---

### Contents

Page

Reference number TECHNICAL REPORT TR 14516 First edition 2002-06-15 Information technology -- Security techniques -- Guidelines for the use and management of Trusted Third Party services Technologies de l'information -- Techniques de sécurité -- Lignes directrices pour l'emploi et la gestion des services TTP PDF disclaimer This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area. Adobe is a trademark of Adobe Systems Incorporated. Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below. or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester. ISO copyright office Case postale 56 · CH-1211 Geneva 20 Tel. + 41 22 749 01 11 Fax + 41 22 749 09 47 E-mail copyright@iso.ch Web www.iso.ch CONTENTS 1 Scope ..... 1

2 References ..... 1

2.1 Identical Recommendations ..... International Standards|1

2.2 Paired Recommendations ..... International Standards equivalent in technical content|1

2.3 Additional References ..... 1

3 Definitions ..... 2

4 General Aspects ..... 3

4.1 Basis of Security Assurance and Trust ..... 3

4.2 Interaction between a TTP and Entities Using its Services ..... 4

4.2.1 In-line TTP Services ..... 4

4.2.2 On-line TTP Services ..... 4

4.2.3 Off-line TTP Services ..... 5

4.3 Interworking of TTP Services ..... 5

5 Management and Operational Aspects of a TTP ..... 5

5.1 Legal Issues ..... 6

5.2 Contractual Obligations ..... 6

5.3 Responsibilities ..... 7

5.4 Security Policy ..... 7

5.4.1 Security Policy Elements ..... 8

5.4.2 Standards ..... 8

5.4.3 Directives and Procedures ..... 8

5.4.4 Risk Management ..... 8

5.4.5 Selection of Safeguards ..... 9

5.4.5.1 Physical and Environmental Measures ..... 9

5.4.5.2 Organisational and Personnel Measures ..... 9

5.4.5.3 IT Specific Measures ..... 9

5.4.6 Implementation Aspects of IT Security ..... 10

5.4.6.1 Awareness and Training ..... 10

5.4.6.2 Trustworthiness and Assurance ..... 10

5.4.6.3 Accreditation of TTP Certification Bodies ..... 11

5.4.7	Operational Aspects of IT Security .....	11
5.4.7.1	Audit/Assessment .....	11
5.4.7.2	Incident Handling .....	12
5.4.7.3	Contingency Planning .....	12
5.5	Quality of Service .....	12
5.6	Ethics .....	12
5.7	Fees .....	12
6	Interworking .....	12
6.1	TTP-Users .....	13
6.2	User-User .....	13
6.3	TTP-TTP .....	13
6.4	TTP-Law Enforcement Agency .....	14
7	Major Categories of TTP Services .....	14
7.1	Time Stamping Service .....	14
7.1.1	Time Stamping Authority .....	14
7.2	Non-repudiation Services .....	15
7.3	Key Management Services .....	16
7.3.1	Key Generation Service .....	16
7.3.2	Key Registration Service .....	16
7.3.3	Key Certification Service .....	16
7.3.4	Key Distribution Service .....	17
7.3.5	Key Installation Service .....	17
7.3.6	Key Storage Service .....	17
7.3.7	Key Derivation Service .....	17
7.3.8	Key Archiving Service .....	17
7.3.9	Key Revocation Service .....	17
7.3.10	Key Destruction Service .....	17
7.4	Certificate Management Services .....	18
7.4.1	Public Key Certificate Service .....	18
7.4.2	Privilege Attribute Service .....	18
7.4.3	On-line Authentication Service Based on Certificates .....	19
7.4.4	Revocation of Certificates Service .....	19
7.5	Electronic Notary Public Services .....	19
7.5.1	Evidence Generation Service .....	20
7.5.2	Evidence Storage Service .....	20
7.5.3	Arbitration Service .....	20
7.5.4	Notary Authority .....	20
7.6	Electronic Digital Archiving Service .....	21
7.7	Other Services .....	22
7.7.1	Directory Service .....	22
7.7.2	Identification and Authentication Service .....	23
7.7.2.1	On-line Authentication Service .....	23
7.7.2.2	Off-line Authentication Service .....	25
7.7.2.3	In-line Authentication Service .....	25
7.7.3	In-line Translation Service .....	25
7.7.4	Recovery Services .....	25
7.7.4.1	Key Recovery Services .....	25
7.7.4.2	Data Recovery Services .....	26
7.7.5	Personalisation Service .....	26
7.7.6	Access Control Service .....	26
7.7.7	Incident Reporting and Alert Management Service .....	26
Annex A - Security Requirements for Management of TTPs .....		28
Annex B - Aspects of CA management .....		29
B.1	Example of Registration Process Procedures .....	29
B.2	An example of requirements for Certification Authorities .....	29
B.3	Certification Policy and Certification Practice Statement (CPS) .....	31

<b>Annex C - Bibliography .....</b>	<b>32</b>
<b>Table of Figures Figure 1 - In-line TTP Service Between Entities .....</b>	<b>4</b>
<b>Figure 2 - On-line TTP Service Between Entities .....</b>	<b>5</b>
<b>Figure 3 - Off-line TTP Service Between Entities .....</b>	<b>5</b>
<b>Figure 4 - Interworking of TTPs in Different Domains .....</b>	<b>13</b>
<b>Figure 5 - Example of Non-repudiation Architecture .....</b>	<b>16</b>
<b>Figure 6 - Link Between an Attribute Certificate and a Public Key Certificate .....</b>	<b>19</b>
<b>Figure 7 - Directory Service Architecture .....</b>	<b>23</b>
<b>Figure 8 - Example for On-line Authentication Services .....</b>	<b>24</b>
<b>Figure 9 - Example for In-line TTP Authentication Service .....</b>	<b>25</b>
<b>Figure 10 - Example of Alert Management Service .....</b>	<b>27</b>