

# ISO/IEC 18014-1:2008-09 (E)

## Information technology - Security techniques - Time-stamping services - Part 1: Framework

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
Introduction .....		v
1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	1
4	Symbols and abbreviated terms .....	4
5	General .....	4
5.1	Background and Summary .....	4
5.2	Services involved in Time-stamping .....	5
5.3	Entities of the Time-Stamping Process .....	5
5.4	Use of Time-Stamps .....	5
5.5	Generation of a Time-Stamp Token .....	6
5.6	Verification of a Time-Stamp Token .....	6
5.7	Time-Stamp renewal .....	6
6	Communications between entities involved .....	7
6.1	Time-Stamp Request Transaction .....	7
6.2	Time-Stamp Verification Transaction .....	8
7	Message Formats .....	8
7.1	Time-stamp request .....	9
7.2	Time-stamp response .....	10
7.3	Time-stamp verification .....	12
7.4	Extension fields .....	12
7.4.1	ExtHash extension .....	12
7.4.2	ExtMethod extension .....	13
7.4.3	ExtRenewal extension .....	13
Annex A (normative) ASN.1 Module for time-stamping .....		14
Annex B (normative) Excerpt of the Cryptographic Message Syntax .....		20
B.1	Introduction .....	20
B.2	General Overview .....	20
B.3	General Syntax .....	20
B.4	Data Content Type .....	21
B.5	Signed-data Content Type .....	21
B.5.1	SignedData Type .....	22
B.5.2	EncapsulatedContentInfo Type .....	23
B.5.3	SignerInfo Type .....	23
B.5.4	Message Digest Calculation Process .....	25
B.5.5	Signature Generation Process .....	25
B.5.6	Signature Verification Process .....	25
B.6	Useful Attributes .....	26
B.6.1	Content Type .....	26

<b>B.6.2</b>	<b>Message Digest .....</b>	<b>26</b>
<b>B.6.3</b>	<b>Countersignature .....</b>	<b>27</b>
	<b>Bibliography .....</b>	<b>28</b>