ISO/IEC TR 29149:2012-03 (E)

Information technology - Security techniques - Best practices for the provision and use of time-stamping services

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Terms and definitions 1

3 Symbols and abbreviated terms 4

4 Time-stamping services 5

5 Use cases for non-repudiation 5
5.1 Introduction 5
5.2 Use case #1 6
5.3 Use case #2 6
5.4 Use case #3 6

6 Potential issues 7
6.1 Security requirements for custody of evidences 7
6.2 Weak cryptography: hash-functions 8
6.3 Weak cryptography: digital signatures 10
6.4 Weak cryptography: message authentication codes 10
6.5 Signature verification 10
6.6 Time-stamp token renewal 11
6.7 Time-stamping service availability 12
6.8 Time-stamping service continuity 12

7 Recommendations 12
7.1 Recommendations for requesters of time-stamp tokens 12
7.2 Recommendations for verifiers of time-stamp tokens 13
7.3 Recommendations for time-stamp service providers 13
7.4 Recommendations for signature verification 16
7.5 Non-repudiation policy 17

8 Algorithms 17
8.1 Overview 17
8.2 Hash functions 17
8.3 Keyed message authentication algorithms 18
8.4 Signature algorithms 18

Bibliography 19