PD ISO/IEC TR 29149:2012

BSI Standards Publication

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

bsi.

...making excellence a habit.™

Document Sharing Hub

National foreword

This Published Document is the UK implementation of ISO/IEC TR 29149:2012.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT - Security techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2012

Published by BSI Standards Limited 2012

ISBN 978 0 580 65106 9

ICS 35.040

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 April 2012.

Amendments issued since publication

Amd. No.	Date	Text affected

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 29149:2012

TECHNICAL REPORT

ISO/IEC TR 29149

First edition
2012-03-15

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

Technologies de l'information — Techniques de sécurité — Meilleures pratiques pour la fourniture et l'utilisation de services d'horodotage

Reference number
ISO/IEC TR 29149:2012(E)

Documents
Document Sharing Hub

© ISO/IEC 2012

Full document details: PD ISO/IEC TR 29149:2012

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2012

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic 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.org
Web www.iso.org

Published in Switzerland

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 29149:2012

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

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 29149:2012

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

In exceptional circumstances, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide to publish a Technical Report. A Technical Report is entirely informative in nature and shall be subject to review every five years in the same manner as an International Standard.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC TR 29149 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

© ISO/IEC 2012 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 29149:2012

Introduction

This Technical Report explains how to provide and use time-stamping services so that time-stamp tokens are effective when used to provide

- timeliness and data integrity services, or
- non-repudiation services (in conjunction with other mechanisms).

ISO/IEC 18014 specifies time-stamping services, explaining how to generate, renew, and verify time-stamp tokens. The goal of a non-repudiation service is to treat evidence concerning a claimed event or action in order to resolve disputes about the occurrence or non-occurrence of the event or action. Depending on the non-repudiation service which is required, the non-repudiation policy in effect for a specific application, and the legal environment within which the application operates, time-stamp tokens from time-stamping authorities may be required as components of non-repudiation information.

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 29149:2012

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

1 Scope

This Technical Report explains how to provide and use time-stamping services so that time-stamp tokens are effective when used to provide timeliness, data integrity, and non-repudiation services in conjunction with other mechanisms. It defines:

— how time-stamp requesters should use time-stamp token generation services;

— how TSAs (time-stamping authorities) should provide a service of guaranteed quality;

— how TSAs should deserve trust based on good practices;

— which algorithms and parameters should be used in TST (time-stamp token) generation and TST renewal, so that TSTs resist during the time period during which the TSTs can be verified as being valid;

— how time-stamp verifiers should use the time-stamp token verification services, both when validating individual TSTs, and when validating sequences of renewal TSTs.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1
certification authority
CA
authority trusted by one or more users to create and assign public-key certificates

NOTE Optionally, the certification authority may create the users' keys.

[ISO/IEC 9594-8:2005]

2.2
digital signature
data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient

[ISO 7498-2:1989]

2.3
evidence
information which is used, either by itself or in conjunction with other information, to establish proof about an event or action

NOTE Evidence does not necessarily prove the truth or existence of something, but can contribute to the establishment of such a proof.

[ISO/IEC 13888-1:2009]

Documents
Document Sharing Hub

© ISO/IEC 2012 – All rights reserved

Full document details: PD ISO/IEC TR 29149:2012

2.4
evidence user
entity that uses non-repudiation evidence

[ISO/IEC 13888-1:2009]

2.5
hash-function
function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties:

— It is computationally infeasible to find for a given output, an input which maps to this output.

— It is computationally infeasible to find for a given input, a second input which maps to the same output.

NOTE Computational feasibility depends on the specific security requirements and environment.

[ISO/IEC 10118-1:2000]

2.6
hash-value
string of bits which is the output of a hash-function

[ISO/IEC 10118-1:2000, modified — The term “hash-code” is used to represent this concept in ISO/IEC 10118-1:2000.]

2.7
imprint
string of bits, either the hash-value of a data string or the data string itself

[ISO/IEC 13888-1:2009]

2.8
message authentication code
MAC
string of bits which is the output of a MAC algorithm

NOTE A MAC is sometimes called a cryptographic check value (see for example ISO 7498-2).

[ISO/IEC 9797-1:2011]

2.9
non-repudiation
ability to prove an action or event has taken place, so that this event or action cannot be repudiated later

[ISO 7498-2:1989]

2.10
non-repudiation token
special type of security token as defined in ISO/IEC 10181-1, consisting of evidence, and, optionally, of additional data

[ISO/IEC 13888-1:2009]

2.11
object identifier
OID
globally unique value associated with an object to unambiguously identify it

[ISO/IEC 8824-1:2002 | ITU X.680:2002]

© ISO/IEC 2012 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 29149:2012