



ICAO

Doc 9303

Machine Readable Travel Documents

Eighth Edition, 2021

Part 13: Visible Digital Seals



Approved by and published under the authority of the Secretary General

INTERNATIONAL CIVIL AVIATION ORGANIZATION



Documents

Document Sharing Hub



| ICAO

Doc 9303

Machine Readable Travel Documents

Eighth Edition, 2021

Part 13: Visible Digital Seals

Approved by and published under the authority of the Secretary General

Published in separate English, Arabic, Chinese, French, Russian
and Spanish editions by the
INTERNATIONAL CIVIL AVIATION ORGANIZATION
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

Downloads and additional information are available at www.icao.int/security/mrtd

Doc 9303, *Machine Readable Travel Documents*
Part 13 — *Visible Digital Seals*
ISBN 978-92-9265-246-3

© ICAO 2020

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, without prior permission in writing from the International Civil Aviation Organization.

AMENDMENTS

Amendments are announced in the supplements to the *Products and Services Catalogue*; the Catalogue and its supplements are available on the ICAO website at www.icao.int. The space below is provided to keep a record of such amendments.

RECORD OF AMENDMENTS AND CORRIGENDA

AMENDMENTS		
No.	Date	Entered by

CORRIGENDA		
No.	Date	Entered by
1	11/12/20	ICAO

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of ICAO concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

TABLE OF CONTENTS

1.	SCOPE	1
2.	DIGITAL SEAL ENCODING	1
2.1	Bar code Format and Print Requirements	1
2.2	Header	3
2.3	Message Zone	4
2.4	Signature Zone	6
2.5	Padding	6
2.6	C40 Encoding of Strings	6
3.	DIGITAL SEAL USAGE	9
3.1	Content and Encoding Rules	9
3.2	Bar code Signer and Seal Creation	9
4.	REFERENCES (NORMATIVE)	11
APPENDIX A TO PART 13 — Exemplary Use Case (informative)		APP A-1
A.1	Prerequisite: Visa Signer Certificate Generation	APP A-2
A.2	Digital Seal Generation	APP A-2
A.3	Digital Seal Validation	APP A-2
APPENDIX B TO PART 13 — Conversion of ECDSA Signature Formats (informative)		APP B-1
B.1	Integer Encoding in BER/DER	APP B-1
B.2	Example	APP B-2
B.2	ECDSA Signatures in ASN.1/DER	APP B-2
APPENDIX C TO PART 13 — Examples for C40 Encoding (informative)		APP C-1
C.1	Example 1	APP C-1
C.2	Example 2	APP C-1
APPENDIX D TO PART 13 — Validation Policy Rules (informative)		APP D-1

1. SCOPE

This Part 13 of Doc 9303 specifies a digital seal to ensure the authenticity and integrity of non-electronic documents in a comparatively inexpensive, but highly secure manner using asymmetric cryptography. The information on the non-electronic document is cryptographically signed, and the signature is encoded as a two-dimensional bar code and printed on the document itself. This approach — the *visible digital seal* — provides the following advantages:

- *Asymmetry*. Due to using asymmetric cryptography, the cost of attaching a digital seal is considerably higher than the cost of issuing a document protected with a digital seal. Thus, even though the cost of issuing a document is very low, it is extremely costly to fake or forge the personalization data of that document.
- *Personalization*. Each digital seal verifies the information printed on the physical document, and is therefore tied to the document holder. There is no direct equivalent of a blank document, therefore no blanks can be lost or stolen.
- *Easy verification*. Even untrained persons are able to verify a document protected with a digital seal by using low-cost equipment, such as an application on a smartphone. Moreover, due to the binary nature of a digital signature, distinguishing between authentic and forged documents is straightforward.

While the digital seal provides a considerable security improvement for (usually paper-based) documents having no microchip, it has considerable limitations when compared to chip-based documents. Storage capacity of digital seals is usually limited to a few kBytes at most and neither the data nor the cryptographic keys or schemes for the digital seal can be updated on existing documents. That is, cryptographic agility is not supported. The digital seal does not provide any protection against cloning, does not implement privacy protection functionality, and is more prone to read errors due to wear and tear than chip-based documents. Furthermore, the versatility of crypto chips allows implementation of additional features, such as signature schemes, terminal authentication, two-factor authentication methods based on shared secrets, i.e. a PIN, or secure cryptographic protocols based on symmetric schemes. As 2D bar codes cannot replace the functional or security features of microchips, travel documents shall employ microchips whenever feasible.

2. DIGITAL SEAL ENCODING

A visible digital seal is a cryptographically signed data structure containing document features, encoded as a 2D bar code and printed on a document. This section provides a description of the encoding and structure of a visible digital seal.

2.1 Bar code Format and Print Requirements

This specification defines how data are encoded into a stream of bytes. Only 2D bar codes whose symbology is specified as an ISO standard SHALL be used. ISO standardized 2D bar codes symbologies include, for example, DataMatrix [ISO/IEC 16022], Aztec Codes [ISO/IEC 24778], and QR Codes [ISO/IEC 18004].

The bar code SHOULD be printed in a way that allows reader equipment (i.e. off-the-shelf smartphones or scanners) to reliably decode the bar code; in particular, [ISO/IEC 15415] SHOULD be taken into account when assessing print quality. The resulting printing and scanning quality requirements depend on the document; application scenario-specific details MAY be specified in a profile. Due to the fact that the quality of printing and scanning affects error rates and influences the robustness of digital seal verification, these quality requirements SHOULD ensure that the bar code containing the

digital seal and all mandatory document features can be reliably verified. Another important requirement addresses symbol contrast of the bar code, because the digital seal might be printed on security paper with a coloured background (e.g. green).

When using standard inkjet printers, it is RECOMMENDED to print with a module size (size of one block of a 2D bar code) of at least 0.3386 mm sidelength per module, corresponding to 4 dots per module sidelength (i.e. 16 dots per module) on a 300 dpi printer, or 8 dots per module sidelength (i.e. 64 dots per module) on a 600 dpi printer. Smaller printing sizes MAY be acceptable, if high-resolution printers or laser printers are used. For the placement of the bar code on the document, see the respective parts of Doc 9303.

The encoded bar code consists of a header (see Section 2.2), message zone (see Section 2.3), and signature zone (see Section 2.4). An overview of the structure is given in Figure 1.

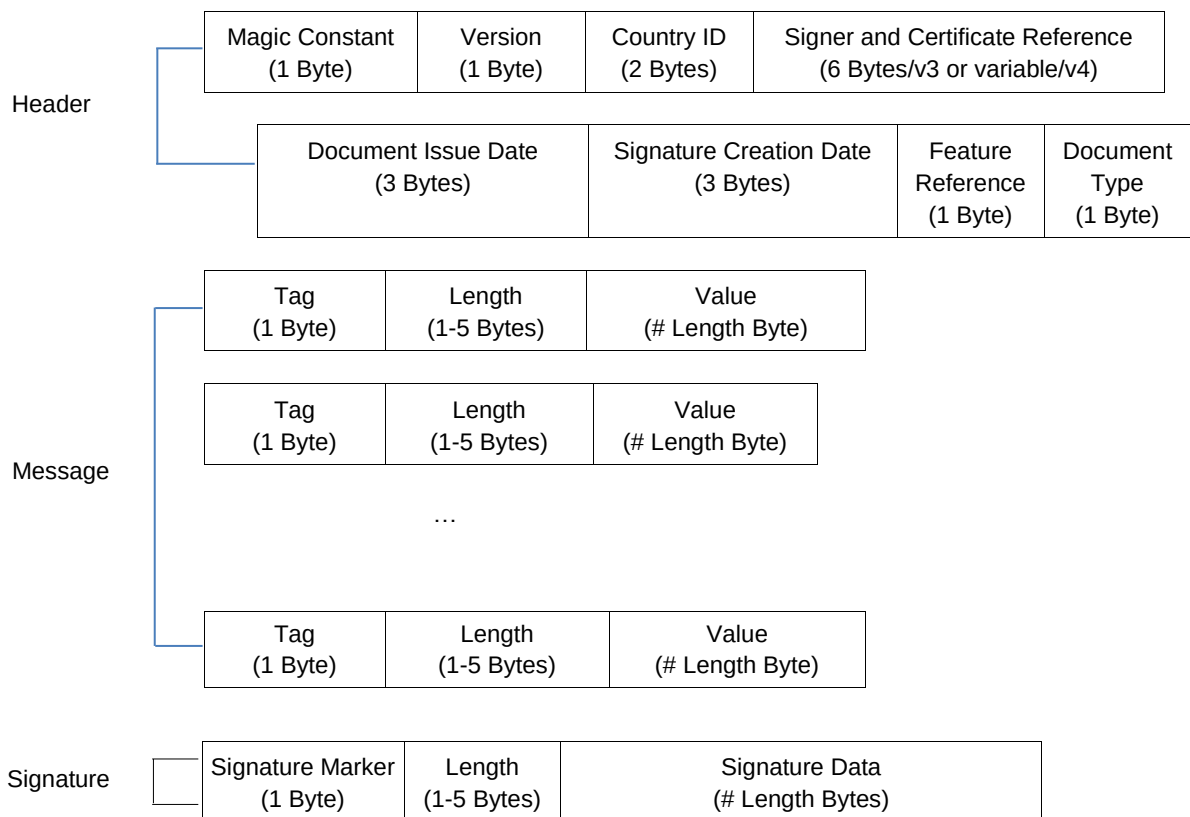


Figure 1. Digital Seal Structure