This is a preview - click here to buy the full publication

## INTERNATIONAL STANDARD

### **ISO/IEC** 20248

First edition 2018-03

# Information technology — Automatic identification and data capture techniques — Data structures — Digital signature meta structure

Technologies de l'information — Techniques d'identification automatique et de capture de données — Structures de données — Méta-structure de signature numérique







#### **COPYRIGHT PROTECTED DOCUMENT**

#### © ISO/IEC 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office CP 401 • Ch. de Blandonnet 8 CH-1214 Vernier, Geneva Phone: +41 22 749 01 11 Fax: +41 22 749 09 47 Email: copyright@iso.org Website: www.iso.org

Published in Switzerland

Introduction	Contents				
1 Scope	Fore	eword		v	
2         Normative references         2           3         Terms and definitions         2           4         Field and data definitions         4           4.1         Field and data definitions         4           4.2         Abbreviations         4           4.2         Abbreviations         5           4.3         Symbols         5           5         Conformance         5           5.1         Specification version         5           5.2         Claiming conformance         5           5.3         Test authority         6           6         DigSig use architecture         6           6.1         General         6           6.2         DigSig Certificate process         7           6.4         DigSig verification process         8           6.5         Error codes         9           7         DigSig Certificate         9           7.1         General         9           7.2         ISO/IEC 20248 Object Identifier         9           7.3         DigSig Certificate pranquere/rise         9           7.4         DigSig crybography         7           7.4.2         Di	Intr	oductio	on	vi	
2   Normative references   2   2   3   Terms and definitions   2   4   Field and data definitions, abbreviations and symbols   4   4.1   Field and data definitions   4   4.2   Abbreviations   4   4.2   Abbreviations   4   4.2   Abbreviations   4   4.3   Symbols   5   5   5   Specification version   5   5.2   Claiming conformance   5.1   Specification version   5   5.2   Claiming conformance   5   5.3   Test authority   6   6   6   6   6   6   6   6   6	1	Scon	ne	1	
Terms and definitions   2		-			
4 Field and data definitions, abbreviations and symbols 4.1 Field and data definitions. 4.2 Abbreviations. 4.3 Symbols. 5 Conformance. 5.1 Specification version 5.2 Claiming conformance. 5.3 Test authority. 6 DigSig use architecture. 6.1 General. 6.2 DigSig Certificate process. 6.3 DigSig generation process. 6.4 DigSig verification process. 6.5 Error codes. 7 DigSig Certificate 9 T.1 General. 9 T.2 ISO/IEC 20248 Object Ideoptifier 9 T.3 DigSig Certificate phrameter use. 7.4 DigSig cryptography. 7.5 DigSig Certificate phrameter use. 7.6 DigSig Certificate phrameter use. 7.7 DigSig Certificate phrameter use. 7.8 DigSig Certificate phrameter use. 7.9 DigSig Certificate phrameter use. 7.1 General. 7.2 DigSig Certificate phrameter use. 7.3 DigSig Certificate phrameter use. 7.4 DigSig cryptography. 7.5 DigSig Domain Authority identifier. 7.6 DigSig Certificate identifier. 7.7 DigSig Syndidy. 7.8 DigSig Certificate identifier. 7.9 DigSig Sertificate identifier. 7.1 Online verificate identifier. 7.2 DigSig Sertificate identifier. 7.3 DigSig Sertificate identifier. 7.4 DigSig Sertificate identifier. 7.5 DigSig Sertificate identifier. 7.6 DigSig Sertificate identifier. 7.7 DigSig Sertificate identifier. 7.8 DigSig Sertificate identifier. 7.9 DigSig Sertificate identifier. 7.10 Online verification. 7.21 General. 7.3 DigSig Sertificate identifier. 7.4 Service did at structures. 7.5 DigSig Sertificate identifier. 7.6 DigSig Sertificate identifier. 7.7 DigSig Sertificate identifier. 7.8 DigSig Sertificate identifier. 7.9 DigSig Sertificate identifier. 7.10 Online verification. 7.11 Online verification. 7.12 Service. 7.13 SigData. 7.14 Service. 7.14 Service. 7.15 SigData. 7.16 Service. 7.17 SigData. 7.18 SigData. 7.19 SigSig Service. 7.10 Online verification. 7.11 SigSig Service. 7.12 SigData. 7.13 SigData. 7.14 Service. 7.15 SigSigSig Service. 7.16 SigSigSigSigSigSigSigSigSigSigSigSigSigS					
4.1       Field and data definitions       4         4.2       Abbreviations       4         4.3       Symbols       5         5       Conformance       5         5.1       Specification version       5         5.2       Claiming conformance       5         5.3       Test authority       6         6       DigSig use architecture       6         6.1       General       6         6.2       DigSig Certificate process       7         6.3       DigSig generation process       8         6.4       DigSig verification process       9         6.5       Error codes       9         7.1       General       9         7.2       ISO/IEC 20248 Object Ideolyfiler       9         7.3       DigSig Certificate       9         7.4       DigSig certificate interpretable       9         7.4       DigSig certificate interpretable       9         7.4       DigSig certificate interpretable       9         7.4.2       DigSig digstall Signatures       10         7.4.2       DigSig digstall Signatures       10         7.5       DigSig Certificate interpretable       10	3	Tern	as and definitions	2	
4.2       Abbreviations       4         4.3       Symbols       5         5       Conformance       5         5.1       Specification version       5         5.2       Claiming conformance       5         5.3       Test authority       6         6.1       General       6         6.1       General       6         6.2       DigSig Certificate process       6         6.3       DigSig gerification process       8         6.4       DigSig verification process       9         6.5       Error codes       9         7       DigSig Certificate       9         7.1       General       9         7.2       ISO/IEC 20%40 Object Identifier       9         7.3       DigSig Certificate parameter use       9         7.4       Digsig chilicate parameter use       9         7.4       Digsig chylography       10         7.4.1       General       10         7.4.2       Digital Separators       10         7.5       Digsig Domain Authority identifier       10         7.6       Digsig Certificate management       12         7.8       Vigsig certifi	4	Field			
4.3       Symbols       5         Conformance       5         5.1       Specification version       5         5.2       Claiming conformance       5         5.3       Test authority       6         5.4       Test specification       6         6       DigSig use architecture       6         6.1       General       6         6.2       DigSig Certificate process       7         6.3       DigSig generation process       7         6.4       DigSig Certificate       9         6.5       Error codes       9         6.5       Error codes       9         7.1       General       9         7.2       ISO/IEC 20248 Object Identifier       9         7.3       DigSig Certificate Process       9         7.4       DigSig cryptography       10         7.4.2       DigSig Certificate Identifier       9         7.4       DigSig Certificate Identifier       10         7.5       DigSig DigSig DigSig Agentificate Identifier       10         7.6       DigSig Certificate Identifier       10         7.6       DigSig Certificate Identifier       10         7.6					
5         Conformance         5           5.1         Specification version         5           5.2         Claiming conformance         5           5.3         Test authority         6           5.4         Test specification         6           6         DigSig use architecture         6           6.1         General         6           6.2         DigSig Certificate process         7           6.3         DigSig generation process         9           6.5         Error codes         9           7         DigSig Certificate         9           7.1         General         9           7.2         ISO/IEC 20248 Object Identifier         9           7.3         DigSig Certificate parameterouse         9           7.4         Objesig Certificate parameterouse         9           7.4         DigSig Certificate parameterouse         9           7.4         DigSig Certificate parameterouse         9           7.4         Digsig Sig Servicontajuets         10           7.5         DigSig Domain Authority identifier         10           7.5         DigSig Domain Authority identifier         10           7.6         DigSig Dom					
5.1       Specification version       5         5.2       Claiming conformance       5         5.3       Test authority       6         5.4       Test specification       6         6       DigSig use architecture       6         6.1       General       6         6.2       DigSig Certificate process       7         6.3       DigSig gerification process       9         6.5       Error codes       9         7       DigSig Certificate       9         7.1       General       9         7.2       ISO/IEC 20248 Object Identifier       9         7.3       DigSig Certificate phrameterouse       9         7.4       DigSig cryptography       10         7.4.1       General       10         7.4.2       Digital Signatures       10         7.4.3       Pivainc containes       10         7.5       DigSig Domain Authority identifier       10         7.5       DigSig Domain Authority identifier       10         7.6       DigSig Certificate ideatrier (CID)       12         7.7       DigSig obtain in the provisition of					
5.2       Claiming conformance       5         5.3       Test authority       6         5.4       Test specification       6         6       DigSig use architecture       6         6.1       General       6         6.2       DigSig Certificate process       7         6.3       DigSig verification process       9         6.4       DigSig Certificate       9         7.5       DigSig Certificate       9         7.1       General       9         7.2       ISO/IEC 20Z48 Object Identifier       9         7.3       DigSig Certificate parameter use       9         7.4       DigSig cryptography       10         7.4.1       General       10         7.4.2       Vigital Signatures       10         7.4.3       Private containers       10         7.5.       DigSig Certificate identifier       10         7.6       DigSig Certificate identifier       10         7.6       DigSig validity       12         7.7       DigSig validity       12         7.8       DigSig validity       12         7.10       Orine verification       13         8	5				
5.3       Test authority       6         5.4       Test specification       6         6.1       General       6         6.2       DigSig Certificate process       7         6.3       DigSig generation process       8         6.4       DigSig verification process       9         6.5       Error codes       9         7       DigSig Certificate       9         7.1       General       9         7.2       ISO/IEC 20248 Object Identifier       9         7.3       DigSig Certificate parameter use       9         7.4       Object Identifier       9         7.4       Digsig Certificate parameter use       9         7.4       Digsig Certificate parameter use       9         7.4       Object Identifier       10         7.4.1       General       10         7.4.2       Digital Signatures       10         7.5       DigSig Domain Authority identifier       10         7.6       DigSig Cortificate identifier (CID)       12         7.7       DigSig cortificate identifier (CID)       12         7.8       DigSig revication       12         7.9       DigSig revication       12<			Specification version	5	
5.4       Test specification       6         6 DigSig use architecture       6         6.1       General       6         6.2       DigSig Certificate process       7         6.3       DigSig generation process       8         6.4       DigSig verification process       9         6.5       Error codes       9         7       DigSig Certificate       9         7.1       General       9         7.2       ISO/IEC 20248 Object Idequifier       9         7.3       DigSig Certificate parameter use       9         7.4       DigSig certificate parameter use       9         7.4       DigSig certificate parameter use       9         7.4       DigSig certificate parameter use       9         7.4.1       General       10         7.4.2       Digital Signatures       10         7.4.3       Private containers       10         7.5       DigSig Certificate detailer (CID)       12         7.5       DigSig Certificate detailer (CID)       12         7.7       DigSig Certificate management       12         7.9       DigSig Vervication       13         8.1       General       14			Claiming conformance	5	
6         DigSig use architecture         6           6.1         General         6           6.2         DigSig Certificate process         7           6.3         DigSig generation process         8           6.4         DigSig verification process         9           6.5         Error codes         9           7         DigSig Certificate         9           7.1         General         9           7.2         ISO/IEC 20248 Object Identifier         9           7.3         DigSig Certificate parameter use         9           7.4         DigSig cryptography         10           7.4         DigSig Certificate parameter use         9           7.4         DigSig Signatures         10           7.4.1         General         10           7.4.2         Digital Signatures         10           7.5         DigSig Domain Authority identifier         10           7.5         DigSig Sertificate identifier (CID)         12           7.7         DigSig Sertificate identifier (CID)         12           7.8         DigSig Sertificate identifier (CID)         12           7.10         Online verification         13           8.1			Test enecification	6	
6.1       General       6         6.2       DigSig Generation process       7         6.3       DigSig generation process       8         6.4       DigSig verification process       9         6.5       Error codes       9         7       DigSig Certificate       9         7.1       General       9         7.2       ISO/IEC 20248 Object Identifier       9         7.3       DigSig Certificate parameter use       9         7.4       DigSig Certificate parameter use       9         7.4       DigSig certificate parameter use       9         7.4       Digsig certificate parameter use       9         7.4.1       General       10         7.4.2       Digital Signatures       10         7.4.3       Private containers       10         7.4.3       Private containers       10         7.5       DigSig Domain Authority identifier       10         7.6       DigSig bomain Authority identifier       10         7.7       DigSig validity       12         7.8       DigSig bertificate management       12         7.9       DigSig validity       12         7.10       Online verification <td>_</td> <td></td> <td>rest specification.</td> <td></td>	_		rest specification.		
6.2       DigSig generation process       7         6.3       DigSig generation process       9         6.4       DigSig verification process       9         6.5       Error codes       9         7       DigSig Certificate       9         7.1       General       9         7.2       ISO/IEC 20248 Object Identifier       9         7.3       DigSig crytificate parameter use       9         7.4       DigSig cryptography       10         7.4.1       Seneral       10         7.4.2       Digstig Signatures       10         7.4.3       Private containers       10         7.5       DigSig Somatures       10         7.6       DigSig validity       12         7.7       DigSig validity       12         7.8       DigSig verocation       12         7.9       DigSig verocation       12         7.10       Orisine verification       13         8       DigSig Data Description (DDD)       13         8.1       General       14         8.2.3       Sigbata       15         8.2.4       DDDdataTagged       15         8.2.5       DDDdataDisplay <td>6</td> <td></td> <td></td> <td></td>	6				
6.3       DigSig generation process       9         6.4       DigSig verification process       9         6.5       Error codes       9         7       DigSig Certificate       9         7.1       General       9         7.2       ISO/IEC 20248 Object Identifier       9         7.3       DigSig certificate parameteruse       9         7.4       DigSig certificate parameteruse       9         7.4       DigSig certificate parameteruse       9         7.4       DigSig certificate parameteruse       9         7.4.1       General       10         7.4.2       DigSig tallianters       10         7.4.3       Private contajores       10         7.5       DigSig bomaba Authority identifier       10         7.6       DigSig certificate identifier (CID)       12         7.7       DigSig validity       12         7.8       DigSig validity       12         7.8       DigSig verificate management       12         7.9       DigSig verificate management       12         7.9       DigSig Data Description (DDD)       13         8.1       General       13         8.2       DDD derived d		_	Ueneral Dig Cortificate process		
6.5 Error codes 9 6.5 Error codes 9 7 DigSig Certificate 9 7.1 General 9 7.2 ISO/IEC 20248 Object Identifier 9 7.3 DigSig Certificate parameter use 9 7.4 DigSig cryptography 10 7.4.1 General 10 7.4.1 General 10 7.4.2 Digital Signatures 10 7.4.3 Private containers 10 7.5 DigSig Domain Authority identifier 10 7.6 DigSig Certificate identifier (CID) 12 7.7 DigSig validity 12 7.8 DigSig Gertificate management 12 7.9 DigSig vertificate management 12 7.9 DigSig vertificate management 13 8 DigSig Data Description (DDD) 13 8.1 General 13 8.2 DDD derived data structures 14 8.2.1 General 14 8.2.2 DDDdata 14 8.2.3 SigData 14 8.2.3 SigData 15 8.2.4 DDDdata 14 8.2.5 DDDdata 15 8.3.6 General 15 8.3.1 General 15 8.3.1 General 16 8.3.2 Sinjps 15 8.3.1 General 16 8.3.3 DigSig format 16 8.3.1 General 17 8.3.3 DigSig format 16 8.3.4 AIDC specific construction of a DigSig 17 8.4 The DigSig physical data path 18 8.5 DDD syntax 20			DigSig generation process	 Ω	
6.5       Error codes       9         7       DigSig Certificate       9         7.1       General       9         7.2       ISO/IEC 20248 Object Identifier       9         7.3       DigSig Certificate parameter rise       9         7.4       DigSig cryptography       10         7.4.1       General       10         7.4.2       Digital Signatures       10         7.4.3       Private containers       10         7.5       DigSig Domain Authority identifier       10         7.6       DigSig certificate identifier (CID)       12         7.7       DigSig validity       12         7.8       DigSig validity       12         7.9       DigSig revocation       12         7.10       Ordine verificate management       12         7.10       Ordine verificate management       12         8.0       DigSig Data Description (DDD)       13         8.1       General       13         8.2       DDD derived data structures       14         8.2.1       General       14         8.2.2       DDDdata and an			DigSig verification process	9	
7         DigSig Certificate         9           7.1         General         9           7.2         ISO/IEC 20248 Object Identifier         9           7.3         DigSig Certificate parameter use         9           7.4         DigSig cryptography         10           7.4.1         General         10           7.4.2         Digital Signatures         10           7.4.3         Private containers         10           7.5         DigSig Domain Authority identifier         10           7.6         DigSig Certificate identifier (CID)         12           7.7         DigSig validity         12           7.8         DigSig Servocation         12           7.9         DigSig validity         12           7.10         Omineverificate management         12           7.10         Omineverification         13           8         DigSig Data Description (DDD)         13           8.1         General         14           8.2.1         General         14           8.2.2         DDD data         15           8.2.4         DDDdataTagged         15           8.2.5         DDDdataTagged         15			Error codes	9	
7.1       General       9         7.2       ISO/IEC 20248 Object Identifier       9         7.3       DigSig Certificate parameter use       9         7.4       DigSig cryptography       10         7.4.1       General       10         7.4.2       DigItal Signatures       10         7.4.3       Private containers       10         7.5       DigSig boman Authority identifier       10         7.6       DigSig validity       12         7.7       DigSig vertificate identifier (CID)       12         7.8       DigSig vertificate management       12         7.9       DigSig vertificate management       12         7.10       Online vertification       13         8       DigSig Data Description (DDD)       13         8.1       General       13         8.2       DDD derived data structures       14         8.2.1       General       14         8.2.2       DDDdata       15         8.2.4       DDDdata       15         8.2.5       DDDdataTalaged       15         8.3       DigSig format       16         8.3.1       General       16         8.3.2 <td>7</td> <td>DiaS</td> <td>ig Cortificato</td> <td>Q</td>	7	DiaS	ig Cortificato	Q	
7.2       ISO/IEC 20248 Object Identifier       9         7.3       DigSig Certificate parameter use       9         7.4       DigSig cryptography       10         7.4.1       General       10         7.4.2       Digital Signatures       10         7.4.3       Private containers       10         7.5       DigSig Dertificate identifier (CID)       12         7.6       DigSig validity       12         7.7       DigSig validity       12         7.8       DigSig validity       12         7.9       DigSig validity       12         7.10       Ordine verificate management       12         7.10       Ordine verification       13         8.1       General       13         8.2       DDD derived data structures       14         8.2.1       General       14         8.2.2       DDDdata       14         8.2.3       SigData       15         8.2.5       DDDdataTagged       15         8.2.5       DDDdataTagged       15         8.2.5       DDDdataTagged       15         8.3.1       General       16         8.3.2       Snips       1	,		General	9	
7.3       DigSig Certificate parameter use       9         7.4       DigSig cryptography       10         7.4.1       General       10         7.4.2       Digital Signatures       10         7.4.3       Private containers       10         7.5       DigSig Domain Authority identifier       10         7.6       DigSig Certificate identifier (CID)       12         7.7       DigSig validity       12         7.8       DigSig validity       12         7.9       DigSig vertificate management       12         7.9       DigSig vertificate management       12         7.10       Online verification       13         8.1       General       13         8.2       DDD derived data structures       14         8.2.1       General       14         8.2.2       DDDdata       14         8.2.3       SigData       15         8.2.4       DDDdataTagged       15         8.2.5       DDDdataTagged       15         8.3.1       General       16         8.3.2       Snips       16         8.3.3       Envelope format       17         8.3.4       AIDC speci			ISO/IEC 20248 Object Identifier	9	
7.4       DigSig cryptography       10         7.4.1       General       10         7.4.2       Digital Signatures       10         7.4.3       Private containers       10         7.5       DigSig bomain Authority identifier       10         7.6       DigSig Certificate identifier (CID)       12         7.7       DigSig Validity       12         7.8       DigSig revocation       12         7.9       DigSig revocation       12         7.10       Onine verification       13         8       DigSig Data Description (DDD)       13         8.1       General       13         8.2       DDD derived data structures       14         8.2.1       General       14         8.2.2       DDD data       15         8.2.3       SigData       15         8.2.4       DDDdataTagged       15         8.2.5       DDDdataDisplay       15         8.3       DigSig format       16         8.3.1       General       16         8.3.2       Snips       16         8.3.3       Envelope format       17         8.4       The DigSig physical data path		7.3	DigSig Certificate parameter use	9	
7.4.3       Private containers       10         7.5       DigSig Doman Authority identifier       10         7.6       DigSig Certificate identifier (CID)       12         7.7       DigSig validity       12         7.8       DigSig Sertificate management       12         7.9       DigSig verocation       12         7.10       Online verification       13         8       DigSig Data Description (DDD)       13         8.1       General       13         8.2       DDD derived data structures       14         8.2.1       General       14         8.2.2       DDDdata       14         8.2.3       SigData       15         8.2.4       DDDdataTagged       15         8.2.5       DDDdataTisplay       15         8.3       DigSig format       16         8.3.1       General       16         8.3.2       Snips       16         8.3.3       Envelope format       17         8.3.4       AIDC specific construction of a DigSig       17         8.4       The DigSig physical data path       18         8.5       DDD syntax       20		7.4	DigSig cryptography	10	
7.4.3       Private containers       10         7.5       DigSig Doman Authority identifier       10         7.6       DigSig Certificate identifier (CID)       12         7.7       DigSig validity       12         7.8       DigSig Sertificate management       12         7.9       DigSig verocation       12         7.10       Online verification       13         8       DigSig Data Description (DDD)       13         8.1       General       13         8.2       DDD derived data structures       14         8.2.1       General       14         8.2.2       DDDdata       14         8.2.3       SigData       15         8.2.4       DDDdataTagged       15         8.2.5       DDDdataTisplay       15         8.3       DigSig format       16         8.3.1       General       16         8.3.2       Snips       16         8.3.3       Envelope format       17         8.3.4       AIDC specific construction of a DigSig       17         8.4       The DigSig physical data path       18         8.5       DDD syntax       20			7.4.1 General	10	
7.5       DigSig Certificate identifier (CID)       10         7.6       DigSig Certificate identifier (CID)       12         7.7       DigSig validity       12         7.8       DigSig Certificate management       12         7.9       DigSig revocation       12         7.10       Online verification       13         8       DigSig Data Description (DDD)       13         8.1       General       13         8.2       DDD derived data structures       14         8.2.1       General       14         8.2.2       DDDdata       14         8.2.3       SigData       15         8.2.4       DDDdataTagged       15         8.2.5       DDDdataDisplay       15         8.3       DigSig format       16         8.3.1       General       16         8.3.2       Snips       16         8.3.3       Envelope format       17         8.3.4       AIDC specific construction of a DigSig       17         8.4       The DigSig physical data path       18         8.5       DDD syntax       20			7.4.2 Digital Signatures	10	
7.6       DigSig Certificate identifier (CID)       12         7.7       DigSig validity       12         7.8       DigSig Certificate management       12         7.9       DigSig revocation       12         7.10       Onkine verification       13         8       DigSig Data Description (DDD)       13         8.1       General       13         8.2       DDD derived data structures       14         8.2.1       General       14         8.2.2       DDDdata       14         8.2.3       SigData       15         8.2.4       DDDdataTagged       15         8.2.5       DDDdataTagged       15         8.3       DigSig format       16         8.3.1       General       16         8.3.2       Snips       16         8.3.3       Envelope format       17         8.3.4       AlDC specific construction of a DigSig       17         8.4       The DigSig physical data path       18         8.5       DDD syntax       20		75	7.4.3 Private comainers	10 10	
7.7       DigSig Validity       12         7.8       DigSig Vertificate management       12         7.9       DigSig revocation       12         7.10       Online verification       13         8       DigSig Data Description (DDD)       13         8.1       General       13         8.2       DDD derived data structures       14         8.2.1       General       14         8.2.2       DDDdata       14         8.2.3       SigData       15         8.2.4       DDDdataTagged       15         8.2.5       DDDdataDisplay       15         8.3       DigSig format       16         8.3.1       General       16         8.3.2       Snips       16         8.3.3       Envelope format       17         8.3.4       AlDC specific construction of a DigSig       17         8.4       The DigSig physical data path       18         8.5       DDD syntax       20			Dig Sig Certificate identifier (CID)	10	
7.8       DigSig Certificate management       12         7.9       DigSig revocation       12         7.10       Online verification       13         8       DigSig Data Description (DDD)       13         8.1       General       13         8.2       DDD derived data structures       14         8.2.1       General       14         8.2.2       DDDdata       14         8.2.3       SigData       15         8.2.4       DDDdataTagged       15         8.2.5       DDDdataDisplay       15         8.3       DigSig format       16         8.3.1       General       16         8.3.2       Snips       16         8.3.3       Envelope format       17         8.3.4       AIDC specific construction of a DigSig       17         8.4       The DigSig physical data path       18         8.5       DDD syntax       20			Digsig validity	12	
79       DigSig revocation       12         7.10       Onkine verification       13         8       DigSig Data Description (DDD)       13         8.1       General       13         8.2       DDD derived data structures       14         8.2.1       General       14         8.2.2       DDDdata       14         8.2.3       SigData       15         8.2.4       DDDdataTagged       15         8.2.5       DDDdataDisplay       15         8.3       DigSig format       16         8.3.1       General       16         8.3.2       Snips       16         8.3.3       Envelope format       17         8.3.4       AIDC specific construction of a DigSig       17         8.4       The DigSig physical data path       18         8.5       DDD syntax       20			DigSig Sertificate management	12	
8       DigSig Data Description (DDD)       13         8.1       General       13         8.2       DDD derived data structures       14         8.2.1       General       14         8.2.2       DDDdata       14         8.2.3       SigData       15         8.2.4       DDDdataTagged       15         8.2.5       DDDdataDisplay       15         8.3       DigSig format       16         8.3.1       General       16         8.3.2       Snips       16         8.3.3       Envelope format       17         8.3.4       AIDC specific construction of a DigSig       17         8.4       The DigSig physical data path       18         8.5       DDD syntax       20		7.9	DigSig revocation	12	
8.1       General       13         8.2       DDD derived data structures       14         8.2.1       General       14         8.2.2       DDDdata       14         8.2.3       SigData       15         8.2.4       DDDdataTagged       15         8.2.5       DDDdataDisplay       15         8.3       DigSig format       16         8.3.1       General       16         8.3.2       Snips       16         8.3.3       Envelope format       17         8.3.4       AIDC specific construction of a DigSig       17         8.4       The DigSig physical data path       18         8.5       DDD syntax       20		7.10	Online verification	13	
8.2       DDD derived data structures       14         8.2.1       General       14         8.2.2       DDDdata       14         8.2.3       SigData       15         8.2.4       DDDdataTagged       15         8.2.5       DDDdataDisplay       15         8.3       DigSig format       16         8.3.1       General       16         8.3.2       Snips       16         8.3.3       Envelope format       17         8.3.4       AIDC specific construction of a DigSig       17         8.4       The DigSig physical data path       18         8.5       DDD syntax       20	8	DigS	ig Data Description (DDD)	13	
8.2.1 General       14         8.2.2 DDDdata       14         8.2.3 SigData       15         8.2.4 DDDdataTagged       15         8.2.5 DDDdataDisplay       15         8.3 DigSig format       16         8.3.1 General       16         8.3.2 Snips       16         8.3.3 Envelope format       17         8.3.4 AIDC specific construction of a DigSig       17         8.4 The DigSig physical data path       18         8.5 DDD syntax       20			General	13	
8.2.2       DDDdata       14         8.2.3       SigData       15         8.2.4       DDDdataTagged       15         8.2.5       DDDdataDisplay       15         8.3       DigSig format       16         8.3.1       General       16         8.3.2       Snips       16         8.3.3       Envelope format       17         8.3.4       AIDC specific construction of a DigSig       17         8.4       The DigSig physical data path       18         8.5       DDD syntax       20		8.2			
8.2.3       SigData       15         8.2.4       DDDdataTagged       15         8.2.5       DDDdataDisplay       15         8.3       DigSig format       16         8.3.1       General       16         8.3.2       Snips       16         8.3.3       Envelope format       17         8.3.4       AIDC specific construction of a DigSig       17         8.4       The DigSig physical data path       18         8.5       DDD syntax       20					
8.2.4       DDDdataTagged       15         8.2.5       DDDdataDisplay       15         8.3       DigSig format       16         8.3.1       General       16         8.3.2       Snips       16         8.3.3       Envelope format       17         8.3.4       AIDC specific construction of a DigSig       17         8.4       The DigSig physical data path       18         8.5       DDD syntax       20					
8.2.5       DDDdataDisplay       15         8.3       DigSig format       16         8.3.1       General       16         8.3.2       Snips       16         8.3.3       Envelope format       17         8.3.4       AIDC specific construction of a DigSig       17         8.4       The DigSig physical data path       18         8.5       DDD syntax       20			8		
8.3       DigSig format       16         8.3.1       General       16         8.3.2       Snips       16         8.3.3       Envelope format       17         8.3.4       AIDC specific construction of a DigSig       17         8.4       The DigSig physical data path       18         8.5       DDD syntax       20			00		
8.3.1 General       16         8.3.2 Snips       16         8.3.3 Envelope format       17         8.3.4 AIDC specific construction of a DigSig       17         8.4 The DigSig physical data path       18         8.5 DDD syntax       20		8.3	1 3		
8.3.3 Envelope format					
8.3.4 AIDC specific construction of a DigSig 17 8.4 The DigSig physical data path 18 8.5 DDD syntax 20			1		
8.4 The DigSig physical data path 18 8.5 DDD syntax 20			1		
8.5 DDD syntax 20		0.1			
· · · · · · · · · · · · · · · · · · ·					
0.0 1/18/18 11101 11/41011 11/5105					
8.7 Data fields 21					

#### ISO/IEC 20248:2018(E)

		8.7.1 Compulsory data fields	21
		8.7.2 Application data fields	
	8.8	Data field object syntax	
	8.9	DDD field types and associate settings	
		8.9.1 General	
		8.9.2 Special field values	
		8.9.3 Field types	
		8.9.4 Special types	29
9	Pragr	mas	29
	9.1	General	
	9.2	entertext	29
	9.3	structjoin	30
	9.4	readmethod	31
	9.5	privatecontainer	32
	9.6	startonword	33
	9.7	cidsniptext	33
Annex	A (no	ormative) Test methods	34
		formative) Example DigSigs	37
			43
		nformative) Typical DigSig EncoderGenerator device architecture	
Annex	E (info	formative) Typical DigSig DecoderVerifier device architecture	48
Annex	F (noi	ormative) DigSig error codes	50
Annex	<b>G</b> (inf	formative) Digital Signature use considerations	52
Annex	<b>H</b> (inf	nformative) Example of a DigSig Certificate	53
Annex	<b>I</b> (info	formative) Example DDD for a physical certificate	54
	-	rmative) DigSig revocation specifications	
		ormative) 2D bar code symbologies — Encoding and decoding the DigSig	
	-	ormative) ISO/IEC 18000-3 Mode 1 RFID protocol and DigSigs	
	-	ormative) ISO/IEC 18000-63 RFID protocol and DigSigs	
	-		
DIDII()	ยาสถกา	nv	80

#### 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 | TC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see <a href="https://www.iso.org/directives">www.iso.org/directives</a>).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see <a href="https://www.iso.org/patents">www.iso.org/patents</a>).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: <a href="https://www.iso.org/iso/foreword.html">www.iso.org/iso/foreword.html</a>.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 31, *Automatic identification and data capture techniques*.



#### Introduction

This document specifies a "language" which is used to specify data constructs with; how the data constructs can be read from one or more AIDC; and how to decode and verify such data.

This document is an ISO/IEC 9594-8 (Public Key Infrastructure: digital signatures and certificates) application specification for automated identification services. Data capacity and/or data transfer capacity of Automated Identification Data Carriers are limited. This restricts the normal use of a digital signature as specified in ISO/IEC 9594-8 within automated identification services.

This document specifies an effective and interoperable method to specify, read, decode and verify data stored in automated identification data carriers, independent from real-time remote control. Meta parameters included in a digital certificate are used to achieve

- offline integrity verification of the data source and data originality,
- a verifiable data structure description to enable interoperability of deployment, domain authority and automated identification data carriers,
- a verifiable data encoding method to achieve compact data to be stored in data constrained automated identification data carriers (the JSON data format is used for both input and output of the encoder and decoder),
- a verifiable automated identification data carrier read method description allowing for the data of a read event to be distributed over more than one carrier of the same and of different technologies, and
- a verifiable method to support key management of cryptographically enabled automated identification data carriers.

The user of this document may use any suitable hashing and asymmetric cryptography method. The choice of cryptography method should be considered carefully and it is advised that only internationally recognized or standardized methods for example FIRS PUB 186-4 and IEEE P1363, be used.

This document should be used in conjunction with standard risk assessments of the use case and environment.

NOTE Many transport applications rely on a secure non-transferable unique identifier to ensure that the data are bound to the tag and/or the vehicle. For such functionality, please refer to ISO/IEC 29167. This specification provides a mechanism to ensure the integrity and authenticity of the data themselves in order to protect against alterations or insertion of alse data into the system. It does not provide any means to defend against replay attacks. Including the secure non-transferable unique identifier of a tag, as signed data, allows for the unrefutable link between the tag and the data and provides a means to determine if the data were read from the tag. The reader can place the read DigSig in another DigSig, effectively signing the read transaction. A third party can then verify that the read transaction happened at a given place and time, as well as the data read.

## Information technology — Automatic identification and data capture techniques — Data structures — Digital signature meta structure

#### 1 Scope

This document is an ISO/IEC 9594-8 (Public Key Infrastructure: digital signatures and certificates) application specification for automated identification services. It specifies a method whereby data stored within a barcode and/or RFID tag are structured, encoded and digitally signed. ISO/IEC 9594-8 is used to provide a standard method for key and data description management and distribution. It is worth noting that the data capacity and/or data transfer capacity of Automated Identification Data Carriers are restricted. This restricts the normal use of a Digital Signature as specified in ISO/IEC 9594-8 within automated identification services.

The purpose of this document is to provide an open and interoperable method, between automated identification services and data carriers, to read data, verify data originality and data integrity in an offline use case.

#### This document specifies

- the meta data structure, the DigSig, which contains the Digital Signature and encoded structured data,
- the public key certificate parameter and extension use, the DigSig Certificate, which contains the
  certified associated public key, the structured data description, the read methods and private
  containers,
- the method to specify, read, describe, sign, verify, encode and decode the structured data, the DigSig Data Description.
- the DigSig EncoderGenerator which generates the relevant asymmetric key pairs, keeps the Private Key secret and generates the DigSigs, and
- the DigSig Decoder Verifier which, by using to the DigSig Certificate, reads the DigSig from the set of Data Carriers, verifies the DigSig and extracts the structured data from the DigSig.

A successful verification of the DigSig signifies the following:

- the data was not tampered with;
- the source of the data is as indicated on the DigSig Certificate used to verify the DigSig with;
- if a secured identifier of the data carrier is included in the DigSig it contains, then the data stored on the data carrier can be considered as the original issued copy of the data; the secure identifier will be able to guarantee that the data carrier is authentic.

This document does not specify

- cryptographic methods, nor
- key management methods.

This document is used in conjunction with standard risk assessments of the use environment.

#### ISO/IEC 20248:2018(E)

#### 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 8824-1<sup>1)</sup>, Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation — Part 1

ISO/IEC 9594- $1^2$ ), Information technology — Open Systems Interconnection — The Directory — Part 1: Overview of concepts, models and services

 $ISO/IEC\ 9594-8^3$ , Information technology — Open Systems Interconnection — The Directory — Part 8: Public-key and attribute certificate frameworks

ISO/IEC 9899, Information technology — Programming languages — C

ISO/IEC 18004, Information technology — Automatic identification and data capture techniques — QR Code bar code symbology specification

ISO/IEC IEEE 9945, Information technology — Portable Operating System Interface (POSIX®) Base Specifications, Issue 7

IETF 3986, Uniform Resource Identifier (URI): Generic Syntax

IETF RFC 5646<sup>4)</sup>, Tags for Identifying Languages

<sup>1)</sup> ITU-T X.680 is equivalent to ISO/IEC 8824-1.

<sup>2)</sup> ITU X.500 is equivalent to ISO/IEC 9594-1, and is the commonly used reference for standard and terminology.

<sup>3)</sup> ITU X.509 is equivalent to ISO/IEC 9594-8, and is the commonly used reference for standard and terminology.

<sup>4)</sup> IEFT RFC 5646 is the reference specification of the IETF BCP 47.