

DIN V 66291-4 :2002-04 (E)

Chip cards with digital signature application/function according to SigG and SigV_- Part_4: Basic security services

Contents

1	Scope.....	3
2	Normative references	3
3	Abbreviations and Notations	5
3.1	Abbreviations	5
3.2	Notations.....	8
4	File Structure	10
5	Global Keys, Global Data and Card Verifiable Certificates.....	11
5.1	Scope.....	11
5.2	Files on MF Level	11
5.3	CV Certificates.....	13
5.4	Reading the Global Data Objects and CV Certificates	13
6	Basic Security Services	14
6.1	Scope.....	14
6.2	Certification Authorities and Certificates	15
6.3	File structure	16
6.4	Application Selection.....	17
6.5	Reading of EF.SSD.....	18
6.6	Authentication of the Cardholder.....	19
6.7	Digital Signature Service.....	20
6.8	Authentication with CV Certificates	27
6.9	Client/Server Authentication.....	32
6.10	Encryption Key Decipherment.....	33
6.11	Reading X.509 Certificates and the Public Key of CAs	37
6.12	Change of Reference Data	38
6.13	Reset of RC and Setting a new PIN or Password	39
7	Cryptographic Token Information	40
7.1	Scope.....	40
7.2	File Structure	40
7.3	Application Selection.....	41
7.4	Reading Cryptographic Token Information.....	41
	Annex A (normative) Digital Signature Formats, AlgIDs and OIDs.....	43
	Annex B (normative) Authentication Certificates	48
	Annex C (normative) File Parameter	57
	Annex D (normative) Device Authentication, Session Key Agreement and Secure Messaging.....	62
	Annex E (normative) Security Service Descriptor Templates	73
	Annex F (informative) ATR-Coding.....	78
	Annex G (informative) Content of Cryptographic Token Information Files.....	81
	Annex H (informative) Identification Data	98
	Annex I (informative) Improvements of DIN V 66291-4 versus DIN V 66291-1	102
	Bibliography	103