

DIN V 66291-3:2003-07 (E)

Chip cards with digital signature application/function according to SigG and SigV_- Part_3: Commands for personalisation

Contents

	Page
1	Scope4
2	Normative references4
3	Abbreviations5
4	Cards with GENERATE ASYMMETRIC KEY PAIR command6
4.1	Pre-Initialisation Phase (V-Phase)6
4.2	Initialisation by the CM (Phase 0).....6
4.2.1	Storage of ICCSN6
4.2.2	Generation of SK.ICC.AUT / PK.ICC.AUT7
4.2.3	Storage of the Certificate C.ICC.AUT8
4.3	Pre-Personalisation Phase (Phase 1)9
4.4	Signature Key Pair Generation (Phase 2).....9
4.4.1	PK Export with SK.ICC.AUT Signature from EF.PK_GEN.....9
4.4.2	PK Export with SM.....11
4.4.3	Generation of AKP and separate export of the PK12
Annex A (normative)	Structure and Content of EF.PK_GEN15
Annex B (informative)	Creation of Files17