

# 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
<b>1 Scope</b> .....	4
<b>2 Normative references</b> .....	4
<b>3 Abbreviations</b> .....	5
<b>4 Cards with GENERATE ASYMMETRIC KEY PAIR command</b> .....	6
4.1 Pre-Initialisation Phase (V-Phase) .....	6
4.2 Initialisation by the CM (Phase 0) .....	6
4.2.1 Storage of ICCSN .....	6
4.2.2 Generation of SK.ICC.AUT / PK.ICC.AUT .....	7
4.2.3 Storage of the Certificate C.ICC.AUT .....	8
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 PK .....	12
<b>Annex A (normative) Structure and Content of EF.PK_GEN</b> .....	15
<b>Annex B (informative) Creation of Files</b> .....	17