

DIN V 66291-2:2003-01 (E)

Chip cards with digital signature application/function according to SigG and SigV_- Part_2:
Personalisation processes

Contents

	Page
1	Scope..... 4
2	Normative references..... 4
3	Terms and definitions 4
3.1	Definitions..... 5
3.2	Abbreviations 7
3.3	Notations..... 7
4	Personalisation models for a ZS..... 9
4.1	Key generation from the smart card's point of view..... 9
4.2	Key generation from the ZS' point of view..... 11
5	Phase model / Lifecycle..... 11
5.1	Pre-initialisation phase 11
5.2	Initialisation phase 12
5.3	Pre-personalisation phase 13
5.4	Key generation phase 13
5.5	Personalisation phase 13
5.6	Operational phase 14
6	Process description of the decentralised model 14
6.1	General requirements 14
6.2	Key generation by the card manufacturer 15
6.3	Key generation by the participant - first personalisation..... 18
6.4	Storage of participant secondary keys into smart cards already used by the participant 21
7	Generation of PK keys at the certification agency, centralised model 23
7.1	Phase 3: Personalisation phase at the certification agency 23
7.2	Phase 4: Operational phase 23
8	Interaction Diagrams..... 24