

Inhaltsverzeichnis

Einleitung	i
1 Software-Qualitätssicherung	1
1.1 Qualitätsmanagement	3
1.2 Qualitätsmanagementmodell des V-Modell	3
1.3 Prozesse der Qualitätssicherung	5
2 Chipkarte als Ausweisdokument	7
2.1 Chipkarten und RFID	9
2.1.1 Bedrohungsszenarien für kontaktlose Chipkarten	9
2.2 Sicherheitsmechanismen nach EAC 1.11	11
2.3 EAC 2.0 konforme Ausweisdokumente	12
2.3.1 Elektronische Authentisierung	12
2.3.2 ePassport-Anwendung	13
2.3.3 eID-Anwendung	13
2.3.4 eSign-Anwendung	14
2.3.5 Zertifikate	14
2.3.6 Password Authenticated Connection Establishment	16
2.3.7 Terminal Authentication	24
2.3.8 Chip Authentication	26
2.3.9 Restricted Identification	27
3 Prüfmethoden	29
3.1 Statische Prüfmethoden	29
3.2 Dynamische Prüfmethoden	31
3.2.1 Strukturorientierte Prüfmethoden	32
3.2.2 Funktionsorientierte Prüfmethoden	33
3.2.2.1 Partitions-Test	34
3.2.2.2 Klassifikationsbaummethode	35
3.2.2.3 Erweiterungen der Klassifikationsbaummethode	37
3.2.2.4 Zustandsbezogener Test	41
3.3 Diversifizierende Prüfmethode	43
3.4 Diskussion	44
4 Prüfstrategie für die Entwicklung von funktionalen Systemtests	47
4.1 Merkmale des Prüflings	48
4.1.1 Untersuchung des Eingaberaumes	49
4.1.2 Chipkartenbetriebssystem abhängige Implementierungsunterschiede	52
4.2 Prüfstrategie	53
4.2.1 Identifikation der Prüfobjekte	55

Inhaltsverzeichnis

4.2.2	Prozessbeschreibung der Prüfung eines Prüfobjekts	55
4.3	Bewertungsmöglichkeiten	58
4.4	Vorteile gegenüber anforderungsbasiertem Test	59
5	Anwendung der Systematik auf Chipkartensoftware von Ausweisdokumenten	61
5.1	Probleme der Testfalldurchführung	61
5.2	Prüfobjektidentifizierung	62
5.3	Modellierung und Testfallableitung der Prüfobjekte	64
5.3.1	PACE	64
5.3.1.1	Verbindungssicht	64
5.3.1.2	Detailsicht	65
5.3.2	Zertifikateinspielung	66
5.3.2.1	Verbindungssicht	67
5.3.2.2	Detailsicht	67
5.3.3	TA/Aux	68
5.3.3.1	Verbindungssicht	68
5.3.3.2	Detailsicht	69
5.3.4	CA	69
5.3.4.1	Verbindungssicht	69
5.3.4.2	Detailsicht	69
5.3.5	Dienstberechtigung	70
5.3.5.1	Verbindungssicht	70
5.3.5.2	Detailsicht	70
6	Erfahrungsbasierter Systemtest	73
6.1	Systematik	73
6.2	Analyse der Testfälle	74
7	Vergleich	77
7.1	Vergleich der Abdeckungsqualität	77
7.2	Vergleich des Aufwands und Wartbarkeit	78
7.3	Zusammenfassung und Ausblick	78
Anhang		81
A	Algorithmus zur Erzeugung von Testimplementierung aus Klassifikationsbäumen	81
B	Zertifikatgenerator	82
C	Beschreibung des Werkzeugs CTE-Export	84
Glossar		85