- ***Prüfungsthemenpaket 1:***
  - Datenschutz und Sicherheitsattribute - **Nr.1 S.3-6**
  - Eigenschaften von Verschlüsselungsalgorithmen - **Nr.1 S.7-9**
  - Signieren und Verschlüsseln von E-Mail - **Nr.2 S.2-4**
  - Identität, Identifikation, Entität, Authentifizierung, Autorisierung - **Nr.2 S.6-8**
- ***Prüfungsthemenpaket 2:***
  - Authentifizierungsverfahren mit Darstellung nach ISO 9798-Notation - **Nr.1 S.12-15**
  - Elektronische Signatur - **Nr.3 S.5-10**
- ***Prüfungsthemenpaket 3:***
  - Padding nach PKCS#1 v1.5 - **Nr.3 S.17**
  - Verzeichnisdienste - **Nr.2 S.10-25**
  - Zertifikatserzeugungs- und Signierungsantrag [CSR]
    - Nr.3 S.24-25
    - (Nr.2 S.5)
- ***Prüfungsthemenpaket 4:***
  - Komponenten einer PKI - **Nr.3 S.2-5**
  - PSE: Personal Security Environment - **Nr.3 S.13**
  - Übersicht PKCS-Standards (PSE) - **Nr.3 S.15-16**
  - PKCS#10 Zertifikatserzeugungs- und Signierungsantrag - **Nr.6-1**
  - HSM-Module - **Nr.3 S.11**
- ***Prüfungsthemenpaket 5:***
  - ASN.1 Notation - **Nr.4**
- ***Prüfungsthemenpaket 6:***
  - Endbenutzerzertifikate und deren Attribute nach X.509 (RFC 5280) ohne Themen im nachfolgenden Paket 7 - **Nr.5 S.2-18**
- ***Prüfungsthemenpaket 7:***
  - Qualifizierte, Attribut- und CA-Zertifikate und deren Attribute nach X.509 (RFC 5280 / RFC 3739,usw) - **Nr.5 S.19-22**
  - Attribut Zertifikate - **Nr.5 S.21-22**
  - Überprüfung der Zertifikatspfade - **Nr.5 S.23-25**
- ***Prüfungsthemenpaket 8:***
  - CRL und OCSP
    - CRL: Nr.7
    - OCSP: Nr.8
- ***Prüfungsthemenpaket 9:***

  - Hashfunktion, MAC und HMAC
    * Hash: Nr.11
    * MAC/HMAC: Nr.12

- ***Prüfungsthemenpaket 10:***
  - Zeitstempel - **Nr.10**
  - Risiken bei Applikationen mit Zertifikaten - **Nr.6**
- ***Prüfungsthemenpaket 11:***
  - Trustketten - **Nr.9 S.2-3**
  - Kreuzzertifizierung - **Nr.9 S.3-5**
  - Trustmodelle - **Nr.9 S.7-11**
  - Zertifikatswechsel bei einer CA - **Nr.9 S.12,16-18**
  - Gültigkeitsmodell Zertifikatsprüfung - **Nr.9 S.13-15**
- ***Prüfungsthemenpaket 12:***
  - SSL/TLS - **Nr.13**
- ***Prüfungsthemenpaket 13:***
  - Kerberos - **Nr. 12.3**
- ***Prüfungsthemenpaket 14:***
  - IPsec ohne Key-Managementprotokolle (Kap. 1 bis und mit Kap. 9.2) - **Nr.14 S.2-26**
- ***Prüfungsthemenpaket 15:***
  - IPsec: Kap. 9.3.1 ISAKMP - **Nr.14 S.27-35**
  - IPsec: Kap. 10 Internet Key Exchange (IKEv1) - **Nr.14 S.36-50**
- ***Prüfungsthemenpaket 16:***
  - IPsec: Kap. 9.3.1 ISAKMP - **Nr.14 S.27-35**
  - IPsec: Kap. 11 Internet Key Exchange Quick Mode (IKEv1) - **Nr.14 S.51-53**
  - IPsec: Kap. 12 NAT-Traversal - **Nr.14 S.54-64**
- ***Prüfungsthemenpaket 17:***
  - IPsec: Kap. 12 NAT-Traversal - **Nr.14 S.54-64**
  - IPsec: Kap. 13 Internet Key Exchange (IKEv2) - **Nr.14 S.65-79**
- ***Prüfungsthemenpaket 18:***
  - Chipkarten - **Nr.15**