Standardisierte TeleSec Smart Cards im Überblick

	TCOS 3.0 min	TCOS 3.0 Signature Card	TCOS 3.0 Signature Card 2.0	NetKey 3.0	IDKey
Betriebsystem					
TCOS 3.0	X	X	X	X	X
Art der Kommunikation					
T=1 (kontaktbehaftet)	X*	X	X*	X	X*
T=1 und T=CL (Dual Interface)	X*		X*		X*
Zugriffskontrolle					
Null-PIN	X**	X	X	X	X
Mehr-PIN	X**	X	X	X	X
Asymmetrische Kryptografie					
RSA mit max. 2048 Bit Schlüsselänge	X	X		X	X
ECDSA mit 256 Bit			X		
ECDH mit 256 Bit			X		
Symmetrische Kryptografie					
DES	X**			X	X
3DES	X**			X	X
IDEA	X**			X	
Applikationen					
SigG mitRSA		X		X	
SigG mit ECC			X		
NKS mit RSA				X	
NKS mit ECC			X		
IDLM					X
Zutritt				X	X
GLAZ				X	X
OTP				X	X
Speichernutzung					
Weitere Applikationen möglich	X	X		X	X
Freier Speicher	X	X		X	X
Evaluierung/Zertifizierung					
Sichere Signatur Erstellungs-einheit (SSEE) gemäß SigG		X	X	X	
Schlüsselmaterial aus T-Systems Trust Center					
2048 Bit RSA(geeignet für qualifizierte Signatur)		X		X	
ECDSA mit 256 Bit (geeignet für qualifizierte Signatur)			X		
2048 Bit RSA (fortgeschritten)				X	X

	TCOS 3.0 min	TCOS 3.0 Signature Card	TCOS 3.0 Signature Card 2.0	NetKey 3.0	IDKey
1024 Bit RSA (fortgeschritten)				X	
ECDSA mit 256 Bit (fortgeschritten)			X		
ECDH mit 256 Bit			X		
Symmetrische Schlüssel				X	X
Bereitstellung von Middleware					
PKCS#11* (Windows/Linux/MacOS/ Android)**		X	X	X	X
-Lotus Notes			****	X	X
-Evidian (ESSO Client PKA V1.2.02)			****	X	X
-CryptoVision			****	X	X
-Mozilla (single Key Zertifikate)			****	X	X
Cardmodul für Microsoft BaseCSP* Windows Vista und folgende			X Nur NKS-Applikation	X Nur NKS-Applikation	X
Signatur, Authentifikation und Verschlüsselung in allen Anwendungen, die Zugriff auf den MS-BaseCSP haben, wie MS-Office, MS-Sharepoint usw.			X****	X	X
MS Identity Lifecycle Management (ILM mit Challenge Response-Verfahren)					X
SSL-LogOn an Web-Applikationen (wenn durch Web-Anwendung unterstützt)			X****	X	X
Cardmanagement-Tool (PIN/PIN2 Handling, Zertifikatsverwaltung)		X	X	X	X

* In Abstimmung mit dem Kunden festzulegen

** Bestandteil des TCOS-Betriebssystems und somit nutzbar

*** PKCS#11 und Microsoft CSP sind offengelegte Programmierschnittstellen zur Integration in Anwendungen

**** Es ist jeweils zu prüfen, ob die Zielanwendung Elliptic Curve Cryptography unterstützt