

## Anlage zu C\_4857 „Stapelsignatur“

Die aktuell definierten Zugriffsregeln für PrK.SAK.AUTD\_CVC.E256 verhindern eine erfolgreiche Stapelsignatur.

### Änderungen in gemSpec\_gSMC-K\_ObjSys:

**Tabelle 107: Tab\_gSMC-K\_ObjSys\_067 Initialisierte Attribute von MF / DF.SAK / PrK.SAK.AUTD\_CVC.E256**

Attribute	Wert	Bemerkung
Objektyp	privates Schlüsselobjekt ELC 256	
keyIdentifier	'0A' = 10	
privateElcKey	domainparameter = brainpoolP256r1	
privateElcKey	keyData = AttributNotSet	wird personalisiert
keyAvailable	Wildcard	
listAlgorithmIdentifier	alle Werte aus der Menge { elcSessionkey4TC }	
accessRulesSessionkeys	Für alle logischen LCS Werte gilt PSO Compute Cryptographic Checksum -> ALWAYS PSO Decipher -> ALWAYS PSO Encipher -> ALWAYS PSO Verify Cryptographic Checksum -> ALWAYS Zugriffsart= PSO à Zugriffsbedingung= AUT(flagTI.52)	
lifeCycleStatus	„Operational state (activated)“	
Zugriffsregel für logischen LCS „Operational state (activated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
ACTIVATE DEACTIVATE	AUT_CMS OR AUT_CUP	
GENERATE ASYMMETRIC KEY PAIR P1='C4' oder P1='C0'	AUT_CMS OR AUT_CUP	siehe Hinweis (114)
GENERATE ASYMMETRIC KEY PAIR P1='81'	PWD(PIN.SAK)	
INTERNAL AUTHENTICATE GENERAL AUTHENTICATE	SmMac(flagTI.52) ALWAYS	siehe Hinweis (113)
DELETE	AUT_CMS OR AUT_CUP	siehe Hinweis (114)
Andere	NEVER	
Zugriffsregel für logischen LCS „Operational state (deactivated)“		
Zugriffsart	Zugriffsbedingung	Bemerkung
Alle	herstellerspezifisch	siehe Hinweis (97)

Anlage zu C\_4857  
„Stapelsignatur“

Zugriffsregel für logischen LCS „Termination state“		
Zugriffsart	Zugriffsbedingung	Bemerkung
Alle	NEVER	