

# Performance von Smart Card Readern



Es ist längst keine Neuigkeit mehr, dass Chipkarten ein wesentlicher und integraler Bestandteil der IT-Security sind. Das zeigen auch die zahlreichen nationalen und internationalen Projekte rund um das Thema eGovernment (Bürgerkarte) und eHealth (Gesundheitskarte). Überall wird eine „smarte“ Karte, meist mit der digitalen Signatur on Board, für die Authentifizierung der Bürger in der digitalen Welt benutzt.

In Österreich zum Beispiel steht neben Master-Card und Maestro-Karte ab Herbst auch die Krankenversichertenkarte („eCard“) als Träger der Bürgerkartenfunktionalität zur Verfügung. Damit sind am Ende dieses Jahres knapp 100 Prozent der österreichischen Bürger mit einer entsprechenden Karte versorgt. Das Freischalten der eCard ist dort sogar ganz ohne zusätzliche Kosten für die Zertifikate vorgesehen. Nachdem auch noch die nötige Software kostenlos zur Verfügung gestellt wird, benötigt man nur noch einen Smart Card Reader, um elektronisch und sicher mit den Behörden in Kontakt treten zu können. Und was im öffentlichen Bereich gilt, hat im Unternehmensumfeld mindestens dieselbe Bedeutung. Banken stellen bereits beim online Banking auf die digitale Signatur als TAN-Ersatz um und viele Unternehmen beseitigen die Probleme rund um Passwörter ein für alle Mal mit einer Mitarbeiterkarte.

Dieser Beitrag soll als Entscheidungshilfe bei der Auswahl von Kartenlesern dienen. Daher wollen wir einen Überblick der am Markt vertretenen Kartenleser bieten, eine Erklärung zu den üblichen Leistungsmerkmalen geben und da Geschwindigkeit auch hier ein ganz wesentlicher Faktor ist, darf eine Performanceauswertung für einige verbreitete Karten auch nicht fehlen.

Beginnen wir mit den wesentlichen Unterscheidungen Anschlussart und Funktion. Es gibt Kartenleser für praktisch alle Anschlüsse am PC, am gängigsten sind jedoch USB, COM und PCMCIA für Notebooks. Da die Datenübertragung zur Karte ebenfalls über ein asynchrones serielles Protokoll mit typischen Geschwindigkeiten zwischen 9,6 und 230 kBit/s, erfolgt, wirkt sich die höhere Übertragungsrates von USB 2.0 in der Endperformance nur vergleichsweise gering aus. Wie wir später auch sehen werden sind die Einflussfaktoren der verwendeten Chipsets und die Implementationen der Treiber im Zusammenspiel mit den Karten von wesentlich größerer Bedeutung.

## Klasse ist klasse

Für die Funktionalität der Kartenleser existiert eine oft verwendete, wenn auch nicht ganz präzise Klassifikation vom ZKA<sup>1</sup> aus Deutschland:

**Klasse 1:** Chipkartenleser der Klasse 1 sind nicht viel mehr als eine Kontaktiereinheit, die über keine weiteren, aus sicherheitstechnischer Sicht relevanten Komponenten verfügen. Ob das Kartenprotokoll selbst vom Reader oder vom PC abgewickelt wird, spielt also keine Rolle.

**Klasse 2:** Leser dieser Klasse verfügen über eine eigene Tastatur oder sind zwischen „normale“ Tastatur und PC eingeschleift. Ziel dieser Maßnahme soll sein, dass Benutzereingaben (z.B. PIN) ohne Umweg über

meintliche Klasse 3 Leser nur als Klasse 2 eingestuft bzw. werden in einem Klasse 2-Modus betrieben.

**Klasse 4:** Leser der Klasse 4 verfügen neben Tastatur und Display noch über ein personalisiertes Sicherheitsmodul mit RSA-Funktionen, um dem jeweiligen Kommunikationspartner zu versichern, dass ein Klasse 4 Terminal eingesetzt wurde. Dadurch ist auch zusätzliche Intelligenz im Terminal nötig.

Darüber hinaus gibt es heute auch Geräte mit Funktionalitäten, die nicht über die Klasespezifikation abgehandelt werden. Hier sei im Speziellen auf Biometriesensorik und kontaktlose Technologie (RFID) verwiesen. Ersteres ist im Besonderen als PIN-Ersatz zur Karte recht interes-

---

„Smart Card Reader  
sind für einen PC das, was  
ein Zylinderschloss für die Haustür ist“

---

den PC zur Karte weitergeleitet werden (Schutz vor Viren und Würmern mit Key-Logger-Funktionalität).

**Klasse 3:** neben Tastatur (wie Klasse 2) verfügen Chipkartenleser dieser Kategorie noch über ein Display, das vom Reader selbst bedient wird. Damit können z.B. Daten von einem Signierprozess noch einmal unverfälscht dargestellt werden. Legt man die Klassifikation genau aus, so kann nur dann von Klasse 3 gesprochen werden, wenn kein Transparent-Mode vorhanden ist, also der PC keinen direkten Einfluss auf die Texte am Display nehmen kann. Dazu muss in den Kartenleser jedoch eine anwendungsspezifische Firmware geladen werden können, da natürlich Karten von verschiedenen Providern unterschiedlich aufgebaut sind. Aus diesem Grund sind auch viele ver-

sant, da hier die zu schützenden Informationen (etwa kryptographische Schlüssel) dezentral und gut gesichert auf der Karte abgelegt sind – Datenschutzbedenken können so einfach aus dem Weg geräumt werden und eine Off-Line-Fähigkeit von einem Serversystem ist auch gegeben. Die Überprüfung des Fingerprints kann auch von der Karte selbst durchgeführt werden (Match-On-Card).

## Standards

Da Smart Cards in vielen unterschiedlichen Bereichen in großer Zahl eingesetzt werden, existieren auch mehrere Standards und Zertifizierungen mit unterschiedlichem Fokus, die zum Teil aber große Überlappung haben. Die „Mutter“ im Kartenbereich ist sicher die interna-



Im Test	Readertyp	ACS		Cherry	Gemplus GemPC		
		ACR 38 U	ACR 30 U	G83-6744 LBZ	Twin Serial	Twin USB	USB-SL
	Firmware Reader	-	-	1.04	V2.00-GF03	V2.00-GT00	V2.00-GT00
	Treiberversion	1.1.4.0	2.1.0.1	1.1.0.32	1.0.5.11	1.0.0.11	1.0.0.11
	Treiberdatum	28.04.04	22.08.03	08.04.05	26.06.04	28.06.04	28.06.04
Readerdetails	Port	USB	USB	USB	Seriell	USB	USB
	Protokolle	T=0/1	T=0/1	T=0/1	T=0/1	T=0/1	T=0/1
	Default CLK (kHz)	4000	3680	4800	4000	4000	4000
	Max. CLK (kHz)	4000	3680	8000	4000	4000	4000
	Default Baudrate (Baud)	9000	9600	10752	10753	10753	10753
	Max. Baudrate (Baud)	344090	9600	412903	344086	344086	344086
	Max. IFSD (Byte)	248	248	254	253	254	253
Treiber	Windows 98	✓	✓		✓	✓	✓
	Windows Me	✓	✓	✓	✓	✓	✓
	Windows 200	✓	✓	✓	✓	✓	✓
	Windows XP	✓	✓	✓	✓	✓	✓
	Windows NT				✓		
	Windows CE				✓	✓	✓
	Linux	✓	✓		✓	✓	✓
	Mac OS X	✓				✓	✓
	PC/SC	✓	✓	✓	✓	✓	✓
	CT-API			✓			
	OCF						
	S=10 (2-wire) SLE 4442	✓	✓	✓	✓	✓	✓
	S=9 (3-wire) SLE 4428	✓	✓	✓	✓	✓	✓
S=8 (12C)	✓	✓	✓	✓	✓	✓	
Zertifizierung	WHQL	✓	✓	✓	✓	✓	✓
	CCID	✓				✓	✓
	EMV	✓	✓	✓	✓	✓	✓
	ITSEC/CC			EAL 3+			
Applikat.	Sichere Digitale Signatur			✓			
	ZKA-Geldkarte						
	Mondex	✓				✓	

## IT SECURITY 6/2005 NOVEMBER/DEZEMBER



Card	Omnikey Cardman				Reiner SCT		SCM			
	3621	3121	3111	4040	pinpad	e-com	SCR531	SCR3310	SPR532	SCR243
2.0	1.01	2.03	2.01	1.00	-	-	4.1.9	5.2	4.21	3.2.0
2.0.0.4	1.1.0.38	1.1.0.38	1.1.0.24	1.1.0.24	0.2.0.0	0.2.0.0	4.27.0.1	4.27.0.1	4.32.0.1	1.20.0.1
14.09.04	19.09.05	19.09.05	11.10.04	11.10.04	20.05.04	20.05.04	11.03.05	11.03.05	28.07.05	29.03.05
PCMCIA	USB	USB	Seriell	PCMCIA	USB	USB	USB	USB	USB/Seriell	PCMCIA
T=0/1	T=0/1	T=0/1	T=0/1	T=0/1	T=0/1	T=0/1	T=0/1	T=0/1	T=0/1	T=0/1
4000	4800	4800	4800	4800	3571	3571	4000	4000	4000	4000
4000	8000	8000	8000	8000	3571	3571	4000	12000	12000	12000
10753	10752	10752	10752	10752	9600	9600	9600	9600	9600	10753
344086	412903	412903	412903	412903	9600	9600	344105	344105	344105	344105
253	254	254	254	254	254	254	252	252	252	252
✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
✓			✓	✓			✓		✓	✓
		✓	auf Anfrage	✓			✓	✓		✓
✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		✓	✓	✓	✓	✓				✓
✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
✓	✓	✓	✓	✓			✓	✓	✓	✓
	✓	✓					✓	✓	✓	
✓	✓	✓	✓	✓			✓	✓	✓	✓
	EAL 3+				E2 hoch	E2 hoch			EAL 3+	
	✓				✓	✓			✓	
						✓				

tionale Norm ISO/IEC 7816 Teil 1 bis mittlerer weile Teil 15. Sie legt alle Merkmale der Karte fest, beginnend mit ihren mechanischen Abmessungen und der elektrischen Belegung der Kontakte, über die An- und Abschaltsequenzen, die Festlegung der Protokollparameter und natürlich auch die Protokolle selbst. Ab Teil 4 aufwärts finden sich vor allem die standardisierten Daten und Kommandos, aber auch neue Technologien im Smart Card Bereich wie USB-Interface oder Biometrieobjekte. Daher muss jeder Kartenleser grundsätzlich zu ISO/IEC 7816<sup>2</sup> Teil 1 bis 3 konform sein. In der Regel ist das auch bei den handelsüblichen Lesern der Fall. Allerdings kann man darauf achten, ob der Reader auch

fischer Treiber installiert werden, sondern jeder CCID-Treiber müsste mit jedem CCID-Leser umgehen können.

### Treiber

Für Smart Card Reader haben sich unterschiedliche nationale und internationale Spezifikationen für deren Einbindung in Systeme mehr oder weniger durchgesetzt. Uneingeschränkte Führungsrolle hat hier ohne jeden Zweifel vor allem auch durch die Initiative von Microsoft der PC/SC<sup>5</sup>-Framework, der von Haus aus in den Windows-Betriebssystemen integriert ist. Er bietet für darauf aufsetzende Anwendungen eine herstellerunabhängige API und unterstützt

von PC/SC, der die Kommunikation zu Lesern von unterschiedlichen Herstellern über eine einzelne Schnittstelle parallel ermöglicht, arbeitet CT-API mit einer vergleichsweise einfachen DLL von jedem Readerhersteller, die direkt von der Anwendung geladen wird. Die CT-API findet gerade im Signaturbereich Anwendung, da hier die Anforderungen nach sicherer PIN-Eingabe über PIN-Pad-Reader besteht und mit dem Teil 4 der MKT (CT-BCS) bereits 1999 eine Spezifikation dafür bestand. PC/SC in der derzeit umgesetzten Version 1.x unterstützt dagegen nur Klasse 1 Funktionalität direkt.

Der Open Card Framework (OCF<sup>6</sup>) geht mit seinem Ziel entscheidend weiter und strebt neben der Kartenterminalunabhängigkeit auch die Abstraktion von Kartenbetriebssystem und Kartenausgeber an. Der Java-Ansatz von OCF konnte sich hierfür jedoch nicht durchsetzen, wodurch deren Bedeutung gering ist.

Im Bereich der Klasse 4 Funktionalität stößt man manchmal auf „finread“<sup>7</sup> welche speziell für die sichere Zahlung und die höchste Stufe der sicheren digitalen Signatur gedacht ist. Weitere Informationen dazu sind im Internet unter dem angegebenen Link zu finden.

### Zertifizierungen

Für die Anwendung der sicheren digitalen Signatur nach Signaturgesetz ist der Einsatz von bestätigten Komponenten erforderlich. Diese werden in Deutschland von der Bundesnetzagentur<sup>8</sup> und in Österreich von der Rundfunk & Telekom Regulierungs GmbH<sup>9</sup> auf ihrer Webseite gelistet. Um diese Bestätigung zu bekommen ist eine genaue Evaluierung der Komponenten nach standardisierten Verfahren vorzulegen. Aus der Homogenisierung einiger nationaler Vorschriften entstand die ITSEC<sup>10</sup>. Für Kartenleser wurde in der Regel die Prüftiefe „E2“ mit der Anforderungsstärke „hoch“ durchgeführt. Der internationale Standard

## „Chipkarten sind für die starke Authentifizierung am besten geeignet.“

alle Spannungsklassen (A' bis C' – entspricht den Versorgungsspannungen von Standard 5 Volt bis zu 1,8 Volt herab) unterstützt.

Aus dem Anwendungsbereich der Kreditkarten kommt die EMV<sup>3</sup>-Spezifikation von Europay, Mastercard und Visa. Diese ist primär als Ergänzung zur ISO/IEC 7816 zu sehen (Börsenfunktionalität, Prüfvorschriften...) – auch wenn sich die beiden in Details widersprechen. Interessant für die Auswahl von Readern ist jedoch eine EMV-Zertifizierung, da hiermit sichergestellt wird, dass sich die Leser in ihren elektrischen Eigenschaften normkonform verhalten (entspricht Level 1).

Bei USB-Lesern findet man auf der USB-Anschlussseite die CCID<sup>4</sup>-Spezifikation (Integrated Circuit(s) Card Interface Devices), welche das Interfacing des Lesers festlegt. Für einen CCID-konformen Kartenleser müsste also kein hardware-spezifi-

Plug & Play. Neben der reinen Kommunikationsfunktionalität zur Karte sind noch Befehle für die Verwaltung von Karten und Leser enthalten. Die Interoperabilität bei PC/SC-Lesern ist in der Regel recht gut, auch wenn es immer wieder Karten gibt, die von manchen Lesern nicht korrekt bedient werden können. Für die Kontrolle der Konformität der PC/SC-Treiber an sich empfiehlt sich auf eine Bestätigung von WHQL (Windows Hardware Quality Labs) zu achten. Detaillierte Informationen zu PC/SC und WHQL findet man auf der Microsoft-Webseite.

Aus dem medizinischen Umfeld in Deutschland stammt eine Schnittstellenspezifikation, die eigentlich nur im deutschsprachigen Raum Verbreitung gefunden hat: das Multifunktionale Kartenterminal (MKT) der TeleTrusT Deutschland e.V., besser bekannt als CT-API (Teil 3 der MKT). Im Gegensatz zum Framework

A-Trust trustsign								
Pos.	Hersteller	Modell	Reset	Kommunikation			Diff. %	Gewichtet
				kurz	mittel	lang		
1	Omniquey	3121	71	6	10	52	0,0	393
2	Reiner SCT	cyberJack pinpad	66	7	11	52	2,5	403
3	Omniquey	3621	68	7	11	55	6,1	417
4	SCM	SCR 3310	62	7	12	66	17,3	461
5	SCM	SPR 532	62	7	12	66	17,3	461
6	SCM	SCR 531	62	7	12	66	17,3	461
7	Omniquey	4040	142	6	11	52	19,6	470
8	ACS	ACR 38 U	68	7	13	66	20,4	473
9	Gemplus	GemPC USB	76	8	12	64	21,1	476
10	Gemplus	GemPC Twin USB	76	8	12	64	21,1	476
11	SCM	SCR 243	66	8	14	68	25,7	494
12	Cherry	G83-6744 LBZ	166	10	16	58	48,6	584
13	Gemplus	GemPC Twin Serial	90	13	20	95	79,9	707
14	Omniquey	3111	285	8	15	74	89,1	743
15	Gemplus	GemPC Card	117	20	39	153	190,8	1143
16	Reiner SCT	cyberJack eCom	400	44	40	166	332,6	1700
17	ACS	ACR 30 U	400	41	55	181	363,9	1823

eCard								
Pos.	Hersteller	Modell	Reset	Kommunikation			Diff. %	Gewichtet
				kurz	mittel	lang		
1	Omniquey	3121	62	4	6	29	0,0	250
2	Reiner SCT	cyberJack pinpad	58	5	6	30	3,6	259
3	ACS	ACR 38 U	57	4	6	35	7,6	269
4	Gemplus	GemPC USB	66	4	6	33	8,0	270
5	Omniquey	3621	62	5	6	32	8,4	271
6	SCM	SCR 531	54	4	7	35	8,8	272
7	SCM	SPR 532	54	4	7	35	8,8	272
8	SCM	SCR 3310	52	4	7	36	9,6	274
9	Gemplus	GemPC Twin USB	66	5	7	33	14,0	285
10	SCM	SCR 243	57	5	8	37	19,2	298
11	Omniquey	4040	133	3	6	29	24,8	312
12	Cherry	G83-6744 LBZ	76	10	10	42	57,6	394
13	Gemplus	GemPC Twin Serial	83	10	15	66	110,8	527
14	Omniquey	3111	285	7	11	54	152,0	630
15	Gemplus	GemPC Card	117	16	28	105	239,6	849
16	Reiner SCT	cyberJack eCom	400	58	83	400	1108,0	3200
17	ACS	ACR 30 U	400	57	95	400	1133,2	3083



## G&amp;D Starcos SPK 2.3

Pos.	Hersteller	Modell	Reset	Kommunikation			Diff. %	Gewichtet
				kurz	mittel	lang		
1	Omniquey	3121	62	6	10	52	0,0	384
2	Reiner SCT	cyberJack pinpad	58	7	11	52	2,9	395
3	Omniquey	3621	58	7	11	55	6,0	407
4	ACS	ACR 38 U	57	7	12	64	16,7	448
5	SCM	SPR 532	54	7	12	66	18,0	453
6	SCM	SCR 531	54	7	12	66	18,0	453
7	SCM	SCR 3310	52	7	12	68	19,5	459
8	Omniquey	4040	133	6	11	52	20,1	461
9	Gemplus	GemPC USB	66	8	12	64	21,4	466
10	Gemplus	GemPC Twin USB	66	8	13	64	22,9	472
11	SCM	SCR 243	57	7	14	68	24,0	476
12	Cherry	G83-6744 LBZ	80	10	15	58	28,1	492
13	Omniquey	3111	285	9	16	80	103,6	782
14	Gemplus	GemPC Twin Serial	83	25	20	95	110,4	808
15	Gemplus	GemPC Card	100	21	35	142	177,9	1067
16	Reiner SCT	cyberJack eCom	400	44	40	166	342,7	1700
17	ACS	ACR 30 U	400	41	55	181	374,7	1823

## Gemplus GemSafeXpresso 32K

Pos.	Hersteller	Modell	Reset	Kommunikation			Diff. %	Gewichtet
				kurz	mittel	lang		
1	Reiner SCT	cyberJack pinpad	55	16	15	19	0,0	365
2	Omniquey	4040	34	20	19	21	12,9	412
3	Omniquey	3121	50	19	19	22	15,9	423
4	ACS	ACR 38 U	43	21	20	24	22,7	448
5	SCM	SPR 532	41	21	21	23	22,7	448
6	SCM	SCR 531	41	21	21	23	22,7	448
7	SCM	SCR 243	40	22	21	22	23,8	452
8	Omniquey	3621	50	20	21	25	24,9	456
9	SCM	SCR 3310	40	21	22	24	25,2	457
10	Gemplus	GemPC Twin USB	54	26	25	27	49,6	546
11	Gemplus	GemPC USB	54	26	26	27	51,2	552
12	Cherry	G83-6744 LBZ	48	25	27	40	63,0	595
13	Omniquey	3111	142	24	26	46	91,2	698
14	Gemplus	GemPC Twin Serial	66	30	31	54	102,2	738
15	Gemplus	GemPC Card	76	38	47	100	201,4	1100
16	ACS	ACR 30 U	86	41	48	100	213,2	1143
17	Reiner SCT	cyberJack eCom	400	54	52	117	356,4	1666

Siemens CardOS 4.3B								
Pos.	Hersteller	Modell	Reset	Kommunikation			Diff. %	Gewichtet
				kurz	mittel	lang		
1	Omnikey	3121	86	5	8	37	0,0	327
2	Reiner SCT	cyberJack pinpad	80	6	9	37	2,8	336
3	SCM	SCR 243	80	6	9	40	6,4	348
4	ACS	ACR 38 U	80	5	8	45	8,0	353
5	Omnikey	3621	86	6	9	41	9,5	358
6	SCM	SPR 531	76	5	9	46	9,8	359
7	SCM	SCR 3310	76	5	9	47	11,0	363
8	SCM	SCR 532	76	5	9	47	11,0	363
9	Gemplus	GemPC USB	90	6	10	45	17,4	384
10	Omnikey	4040	153	4	8	37	17,7	385
11	Gemplus	GemPC Twin USB	90	7	10	45	20,2	393
12	Reiner SCT	cyberJack eCom	66	7	11	52	23,2	403
13	Cherry	Smartboard	100	11	14	47	44,0	471
14	Omnikey	3111	333	9	15	74	144,6	800
15	Gemplus	GemPC Twin Serial	105	13	60	76	170,9	886
16	Gemplus	GemPC Card	133	20	30	117	193,9	961
17	ACS	ACR 30 U	400	40	47	166	421,7	1706

Telesec TCOS 2.0								
Pos.	Hersteller	Modell	Reset	Kommunikation			Diff. %	Gewichtet
				kurz	mittel	lang		
1	Omnikey	3121	68	7	10	51	0,0	395
2	Reiner SCT	cyberJack pinpad	62	8	11	52	3,3	408
3	Omnikey	3621	64	8	11	52	3,8	410
4	SCM	SPR 532	57	8	12	62	13,7	449
5	SCM	SCR 531	57	8	12	62	13,7	449
6	SCM	SCR 3310	57	8	12	62	13,7	449
7	Omnikey	4040	133	7	10	48	13,4	448
8	ACS	ACR 38 U	58	8	11	60	10,4	436
9	Gemplus	GemPC USB	68	9	12	60	16,7	461
10	Gemplus	GemPC Twin USB	68	9	12	60	16,7	461
11	SCM	SCR 243	58	9	13	62	17,7	465
12	Cherry	G83-6744 LBZ	80	10	17	83	52,9	604
13	Gemplus	GemPC Twin Serial	83	14	19	105	88,1	743
14	Omnikey	3111	285	10	15	74	92,7	761
15	ACS	ACR 30 U	400	40	55	0	175,9	1090
16	Gemplus	GemPC Card	111	21	36	166	198,7	1180
17	Reiner SCT	cyberJack eCom	400	43	40	181	343,3	1751



ISO/IEC 15408 löste mit seinen „Common Criteria“ (CC) die ITSEC-Methodik gewissermaßen ab. Eine vergleichbare Prüftiefe wird bei CC mit EAL3 erzielt. Auf diese Angaben sollte bei Klasse 2 und Klasse 3 Geräten, welche für die sichere digitale Signatur eingesetzt werden, geachtet werden. Grundsätzlich sollte jedoch der Empfehlung des Trust Centers folge geleistet werden.

**Der Test**

Wir haben für Sie 17 Produkte von Klasse 1 bis Klasse 3, von PCMCIA bis USB auf ihre Performance hin getestet und dabei natürlich auf die Verfügbarkeit von Treibern und Zertifizierungen geachtet. Dabei haben wir jeweils die aktuellen Produkte der Hersteller und die letzten verfügbaren Treiberstände verwendet. In der Tabelle 1 finden Sie einen Überblick über die getesteten Leser und deren Funktionalität. Im Bereich der Readerdetails werden jene Parameter angeführt, die vom Lesertreiber zurückgemeldet werden, allerdings wurden sie nicht auf ihre Richtigkeit hin geprüft. Die Verfügbarkeit der Treiber richtete sich nach der Möglichkeit des freien Downloads von der Webseite des Herstellers zum Zeitpunkt des Tests. Ebenso wurden die dort getätigten Angaben über die erlangten Zertifizierungen übernommen, ohne jede Angabe zu kontrollieren.

Bei der Analyse der Readerperformance stellten wir fest, dass das Ranking stark von der getesteten Karte abhängig ist. Einerseits ist dies klar, weil die Karte gibt dem Kartenleser nach einem Reset in der ATR (Answer To Reset) die unterstützten Kommunikationsparameter mit. Es liegt dann also in der Hoheit des Lesers, auf welche Parameter er die Karte umschaltet und damit wird in Folge die Kommunikationsgeschwindigkeit zwischen Karte und Leser bestimmt. Andererseits waren auch wir überrascht, dass manche Karten bei manchen Readern um einen Faktor 11 (!) langsamer waren

**Die Links der getesteten Produkte**

Die getesteten Produkte im Überblick (weitere Informationen dazu finden Sie im angegebenen Link):

**KLASSE 1 – USB**

ACS ACR 30U	<a href="http://www.cryptoshop.com/index.php?r=ACR30U">www.cryptoshop.com/index.php?r=ACR30U</a>
ACS ACR 38U	<a href="http://www.cryptoshop.com/index.php?r=ACR38U">www.cryptoshop.com/index.php?r=ACR38U</a>
GEMPLUS GemPC Twin USB	<a href="http://www.cryptoshop.com/index.php?r=TwinUSB">www.cryptoshop.com/index.php?r=TwinUSB</a>
GEMPLUS GemPC USB-SL	<a href="http://www.cryptoshop.com/index.php?r=GemPCUSB">www.cryptoshop.com/index.php?r=GemPCUSB</a>
OMNIKEY Cardman 3121	<a href="http://www.cryptoshop.com/index.php?r=CM3121">www.cryptoshop.com/index.php?r=CM3121</a>
SCM SCR 3310	<a href="http://www.cryptoshop.com/index.php?r=SCR3310">www.cryptoshop.com/index.php?r=SCR3310</a>
SCM SCR 531	<a href="http://www.cryptoshop.com/index.php?r=SCR531">www.cryptoshop.com/index.php?r=SCR531</a>

**KLASSE 1 – COM**

GEMPLUS GemPC Twin SL	<a href="http://www.cryptoshop.com/index.php?r=TwinSER">www.cryptoshop.com/index.php?r=TwinSER</a>
OMNIKEY Cardman 3111	<a href="http://www.cryptoshop.com/index.php?r=CM3111">www.cryptoshop.com/index.php?r=CM3111</a>

**KLASSE 1 – PCMCIA**

GEMPLUS GemPC Card	<a href="http://www.cryptoshop.com/index.php?r=GemPCCard">www.cryptoshop.com/index.php?r=GemPCCard</a>
OMNIKEY Cardman 4040	<a href="http://www.cryptoshop.com/index.php?r=CM4040">www.cryptoshop.com/index.php?r=CM4040</a>
SCM SCR 243	<a href="http://www.cryptoshop.com/index.php?r=SCR243">www.cryptoshop.com/index.php?r=SCR243</a>

**KLASSE 2**

CHERRY G83-6744 LBZ (Tastatur)	<a href="http://www.cryptoshop.com/index.php?r=G83-6744">www.cryptoshop.com/index.php?r=G83-6744</a>
OMNIKEY Cardman 3621	<a href="http://www.cryptoshop.com/index.php?r=CM3621">www.cryptoshop.com/index.php?r=CM3621</a>
REINER SCT pinpad	<a href="http://www.cryptoshop.com/index.php?r=CJPinPad">www.cryptoshop.com/index.php?r=CJPinPad</a>
SCM SPR 532	<a href="http://www.cryptoshop.com/index.php?r=SPR532">www.cryptoshop.com/index.php?r=SPR532</a>

**KLASSE 3**

REINER SCT e-com	<a href="http://www.cryptoshop.com/index.php?r=e-com">www.cryptoshop.com/index.php?r=e-com</a>
------------------	--

Testen Sie Ihren Reader online unter [www.cryptoshop.com/readertest](http://www.cryptoshop.com/readertest)



Tabelle : Überblick über die getesteten Leser und deren Funktionalität.

als mit dem schnellsten Leser des Tests. Aber selbst Geschwindigkeitsunterschiede von 30 % können bei Transaktionszeiten von mehreren Sekunden bei regelmäßigem Gebrauch störend auffallen.

Der Test bestand aus vier Teilen: Kartenreset und die Übertragung von drei unterschiedlich langen Kommandos zur Karte (7, 32 und 256 Byte lang). Dabei wurde die jeweilige Dauer des Teilergebnisses über

eine Zeit von 2 Sekunden gemittelt, die Angaben sind jeweils in Millisekunden. Unser Performanceindikator wurde als gewichtete Summe der Teilergebnisse so gewählt, dass er üblichen Kartentransaktionen möglichst nahe kommt. Je kleiner die Zahlen, desto schneller sind somit die Leser.

Es war auch zu beobachten, dass die Geschwindigkeit erheblich von der Anzahl der installierten Treiber (unser Test bezieht sich ausschließlich auf PC/SC) abhängig war. Um somit gleiche Bedingungen für die getesteten Produkte zu schaffen, wurden alle 17 Leser parallel betrieben. Das hat zwar die absoluten Werte verschlechtert, jedoch die Vergleichbarkeit wesentlich gesteigert. Natürlich hängt die ermittelte Geschwindigkeit auch von der Rechenleistung des Test-PCs ab. Um Ihnen auch einen Test Ihrer Kartenleser mit Ihren eigenen Karten zu ermöglichen, haben wir unter [www.cryptoshop.com/readertest](http://www.cryptoshop.com/readertest) ein Service eingerichtet, mit dem Sie das sicher und

einfach online erledigen können. Unter dieser Adresse finden Sie auch weitere getestete Karten, ausführlichere Ergebnisse und Analysen.

### Fazit

Wie in vielen Bereichen ist die „richtige“ Wahl sehr stark von der eigenen Anwendung und deren Anforderungen abhängig. Im konkreten Fall hat allerdings auch die eingesetzte Karte einen großen Einfluss auf die resultierende Übertragungsgeschwindigkeit. Der Grund dafür liegt in den Tiefen der Übertragungsparameter, die in der ATR von der Karte bekannt

gegeben werden. Für Kartenausgeber, die auf diese Faktoren durchaus Einfluss nehmen können, bedeutet dies, dass es zu einem großen Teil in ihrer Hand liegt, wie schnell das System im Endeffekt arbeitet. Auch wenn die Rahmenbedingungen zu einem scheinbar langsameren Leser zwingen, besteht immer noch die Möglichkeit über eine optimierte ATR die Gesamtleistung zu verbessern!



Stefan Bumerl  
stefan.bumerl@  
cryptas.com

- 
- 1 Zentraler Kreditausschuss, weitere Informationen sind unter [www.zka.de](http://www.zka.de) erhältlich
  - 2 Siehe auch [www.iso.ch](http://www.iso.ch)
  - 3 Siehe auch [www.emvco.com](http://www.emvco.com)
  - 4 Siehe auch [www.usb.org](http://www.usb.org)
  - 5 Siehe auch [www.pcscworkgroup.com](http://www.pcscworkgroup.com)
  - 6 Siehe auch [www.opencard.org](http://www.opencard.org)
  - 7 Siehe auch [www.cenorm.be/iss/workshop/finread/default.htm](http://www.cenorm.be/iss/workshop/finread/default.htm)
  - 8 Siehe auch [www.bundesnetzagentur.de](http://www.bundesnetzagentur.de)
  - 9 Siehe auch [www.rtr.at](http://www.rtr.at)
  - 10 Siehe auch [www.bsi.de/zertifiz/itkrit/itsec-dt.pdf](http://www.bsi.de/zertifiz/itkrit/itsec-dt.pdf)