



## Zentrum für sichere Informationstechnologie – Austria Secure Information Technology Center – Austria

A-1040 Wien, Weyringergasse 35  
Tel.: (+43 1) 503 19 63-0  
Fax: (+43 1) 503 19 63-66

A-8010 Graz, Inffeldgasse 16a  
Tel.: (+43 316) 873-5514  
Fax: (+43 316) 873-5520

<http://www.a-sit.at>  
E-Mail: [office@a-sit.at](mailto:office@a-sit.at)

DVR: 1035461

ZVR: 948166612

# LEITFADEN ZUR SICHEREN VERWENDUNG VON CHIPKARTEN-LESERN

Autor – [Herbert.Leitold@a-sit.at](mailto:Herbert.Leitold@a-sit.at)

**Zusammenfassung:** Im Einsatz von Chipkarten – etwa als Bürgerkarte – sind AnwenderInnen mit der Frage konfrontiert, welche Kartenleser sinnvoll sind. Am Markt sind durch die zunehmende Verbreitung bereits recht günstige einfache Geräte verfügbar, oft sind Kartenleser bereits in PCs oder Laptops eingebaut. Dem stehen Kartenleser mit eigener Tastatur und teils auch eigener Anzeige gegenüber, die dann deutlich höhere Preise haben. Für die Verwendung in sensiblen Bereichen wie für qualifizierte Signaturen im E-Government oder im Internet-Banking ist für AnwenderInnen neben den Anschaffungskosten auch die Sicherheit ein wesentliches Kriterium. Es ist dabei für die breite Masse oft schwer zu bewerten, ob mit der Anschaffung günstigerer Kartenleser zusätzliche Risiken bestehen.

Um der breiten Öffentlichkeit eine Hilfestellung und auch Handlungsempfehlungen zu geben, soll deshalb dieses Dokument die Situation allgemein verständlich erklären. Es wird die Technologie der elektronischen Signatur kurz erläutert. Theoretische Restrisiken auch bei Einsatz von modernsten Chipkarten werden beschrieben und es werden Empfehlungen gegeben, damit diese Restrisiken nicht zum Schaden der AnwenderInnen durch Angreifer auch praktisch ausgenutzt werden können.

Das Dokument beschränkt sich dabei auf den Anwendungsfall qualifizierte Signatur als dem elektronischen Äquivalent zur handschriftlichen Unterschrift. Es ist aber sinngemäß auch auf andere Anwendungsfälle von Chipkarte und PIN anwendbar.

## Inhaltsverzeichnis

Inhaltsverzeichnis	1
1. Ausgangssituation	1
2. Problembeschreibung	2
2.1. Grundlagen der qualifizierten Signatur	2
2.2. Das System Karte – Leser – Software	2
3. Typen von Kartenlesern	3
4. Angriffsmöglichkeiten	4
4.1. Theoretische Angriffsszenarien	4
4.2. Praktische Relevanz	5
4.3. Kartenleser vs. Angriffsmöglichkeiten	5
5. Schlussfolgerungen	6
6. Handlungsempfehlungen	7

## 1. Ausgangssituation

Das österreichische Signaturgesetz (SigG) bzw. die Signaturverordnung (SigV) – nunmehr Signaturverordnung 2008 (SigV 2008) regeln seit dem Jahr 2000 die Gleichstellung von so genannten *qualifizierten Signaturen*<sup>1</sup> mit einer händischen Unterschrift. Österreich hat damit als erster die Signaturrechtlinie der EU umgesetzt und zählt seither in der Anwendung und Verbreitung elektronischer Signaturen zu den Vorreitern in Europa. Zur Gewährleistung der technischen Sicherheit werden technische Komponenten laufend am Stand der Technik geprüft – es werden Bescheinigungen ausgestellt, die unter anderem von A-SIT als

<sup>1</sup> Qualifizierte Signaturen wurden vor der aktuellen Version des SigG (Novelle BGBl. I 8/2008) als „sichere elektronische Signaturen“ bezeichnet. Dieses Dokument verwendet durchgängig den aktuellen Begriff „qualifizierte Signatur“, dies ist synonym zu sicheren elektronischen Signaturen zu sehen.

Bestätigungsstelle ausgefertigt werden. Komponenten werden dabei strengen technischen Tests unterzogen – bei aktuell in Österreich eingesetzten Systemen meist von Evaluierungsstellen in Deutschland, international anerkannte Zertifikate zu Evaluierungen werden etwa vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) ausgestellt.

Wurden anfangs für qualifizierte Signaturen mehrere Komponenten wie Software oder Kartenleser einer Bescheinigung unterzogen, so hat 2004 eine Novelle der SigV<sup>2</sup> bzw. dann auch 2008 des SigG bzw. SigV<sup>3</sup> klargestellt, dass die Bescheinigungspflicht sich nur auf jene Komponenten beschränkt, die die so genannten Signaturerstellungsdaten halten oder diese verarbeiten – das ist in der Praxis die Chipkarte, wie die e-card oder eine Bankomatkarte als Bürgerkarte.

Für AnwenderInnen aber auch für Anwendungsbetreiber entsteht zeitweise Verunsicherung, welche Kartenleser für qualifizierte Signaturen zulässig oder hinreichend sicher sind. Ohne auf allfällige privatrechtliche Regelungen zwischen Signator<sup>4</sup> und dem Zertifizierungsdiensteanbieter (ZDA)<sup>5</sup> einzugehen, wird deshalb in diesem Dokument beschrieben, welche Vorkehrungen zu treffen sind, damit Kartenleser entsprechend sicher eingesetzt sind.

## 2. Problembeschreibung

### 2.1. Grundlagen der qualifizierten Signatur

Elektronische Signaturen basieren auf der so genannten asymmetrischen Kryptographie. Dabei teilt sich der kryptographische Schlüssel in einen privaten und einen öffentlichen Schlüssel. Die Sicherheit basiert darauf, dass der private Schlüssel zur Erstellung der Signatur<sup>6</sup> geheim gehalten wird. Der öffentliche Schlüssel zur Signaturprüfung<sup>7</sup> kann hingegen bekannt gemacht werden und wird vom ZDA mit einem Zertifikat als zum privaten Schlüssel des Signator gehörig bestätigt.

Damit der private Schlüssel auch geheim bleibt, wird er in Chipkarten gehalten. Moderne Chipkarten erzeugen den privaten Schlüssel in der Karte<sup>8</sup> und der Schlüssel verlässt die Karte nie. Auch die kryptographischen Berechnungen für die Anwendung des Schlüssels erfolgen in der Chipkarte. Unter den strengen Sicherheitsanforderungen der qualifizierten Signatur ist davon auszugehen, dass die Chipkarten am höchsten Stand der Technik sicher sind.

Zur Sicherheit der qualifizierten Signatur gehört auch, dass deren Auslösung nur durch den Signator erfolgen und willentlich erfolgen kann. Dazu muss vor der Auslösung zwingend ein Autorisierungscode des Signators eingegeben werden – in der Praxis sind das PINs.

### 2.2. Das System Karte – Leser – Software

Aus den beiden grundlegenden Sicherheitsanforderungen der qualifizierten Signatur – dass der private Schlüssel die Chipkarte nie verlässt und dass ein Autorisierungscode einzugeben ist – folgt, dass sowohl das zu signierende Dokument, als auch die PIN an die Chipkarte „herangeführt“ werden müssen. Wesentliche Komponenten sind dabei:

---

<sup>2</sup> Signaturverordnung BGBl. II Nr. 527/2004

<sup>3</sup> Signaturgesetz BGBl. I Nr. 8/2008 bzw. Signaturverordnung BGBl. II Nr. 3/2008

<sup>4</sup> Wurde bisher von AnwenderIn als der Person, die mit der Chipkarte eine Signatur auslöst, gesprochen, wird in Folge der dafür im SigG festgelegte Begriff „Signator“ verwendet.

<sup>5</sup> Zum Zeitpunkt der Erstellung dieses Dokuments ist die Firma A-Trust der einzige ZDA in Österreich, der qualifizierte Zertifikate für qualifizierte Signaturen ausstellt. Die grundsätzlichen technischen Überlegungen dieses Dokuments sind jedoch vom ZDA im Wesentlichen unabhängig.

<sup>6</sup> auch als „Signaturerstellungsdaten“ bezeichnet

<sup>7</sup> auch als „Signaturprüfdaten“ bezeichnet

<sup>8</sup> Auf Fälle, wo im Produktionsprozess der Chipkarte Schlüssel z.B. in speziellen Modulen erzeugt und sicher auf die Chipkarte aufgebracht werden, wird hier nicht eingegangen. Es kann aber auch hier von entsprechend sicherem Handling der Schlüssel ausgegangen werden.

- Eine Softwarekomponente die das zu signierende Dokument anzeigt und aufbereitet<sup>9</sup>. Für die Bürgerkarte ist das etwa eine Bürgerkartenumgebung.
- Ein Kartenleser als physikalische Schnittstelle samt Treiber als logische Schnittstelle zwischen PC/Laptop und Chipkarte.
- Eine Komponente zur PIN-Eingabe. Diese kann – je nach Kartenleser und dessen Treiber – Teil der Signatursoftware, des Treibers, oder des Kartenlesers sein
- Die Chipkarte selbst

Diese Komponenten und ihr Zusammenspiel werden im folgenden Schaubild schematisch dargestellt. Unterschreibt ein Signator ein Dokument, so wird durch die Signatursoftware der Hash-Wert gebildet und via Kartenleser an die Chipkarte übermittelt. Der Signator gibt die PIN – je nach Kartenleser an diesem, in einer Anzeige des Treibers oder in der Signatursoftware ein. Die Chipkarte vergleicht dann die PIN auf Richtigkeit und erstellt die Signatur über Anwendung des privaten Schlüssels auf den Hash-Wert.

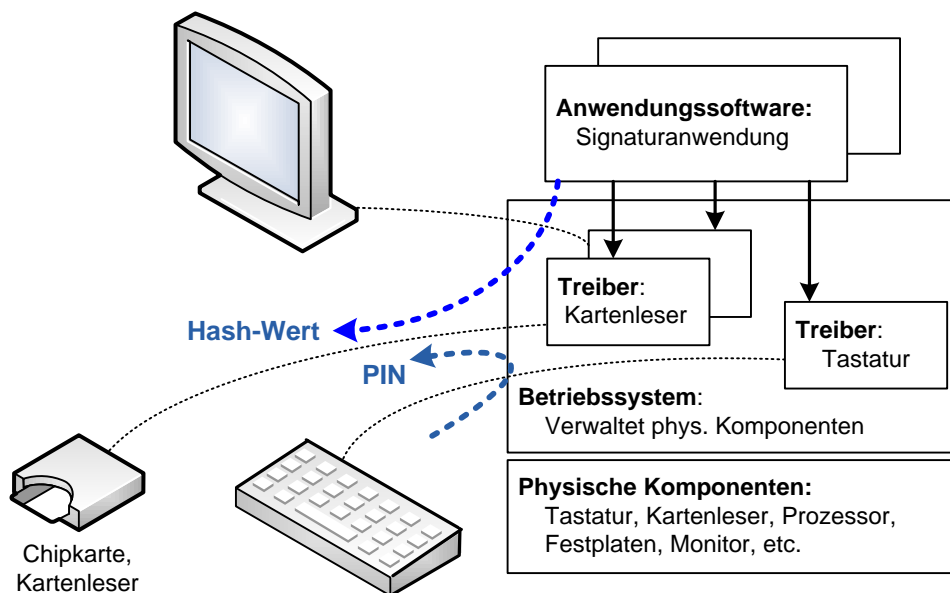


Abbildung 1: System Software – Treiber – Karte – Leser  
(hier Kartenleser ohne PIN-Pad)

### 3. Typen von Kartenlesern

Die am Markt verfügbaren Kartenleser sind vielfältig. Es bestehen solche, die am USB-Board angesteckt werden, in den PCMCIA-Slot des Laptops gesteckt werden, können auch in die PC-Tastatur integriert, oder bereits integrierter Teil des PCs oder Laptops sein.

Hinsichtlich der Sicherheit ergeben sich Unterschiede vor allem daraus, welche Funktionen die Kartenleser selbst zur Verfügung stellen. Im deutschen Sprachraum wird oft auf eine Einteilung in vier Sicherheitsklassen bezogen, die auf der HBCI-Spezifikation für Internet-Transaktionen mit der deutschen Geldkarte basiert<sup>10</sup>:

- **Klasse 1:** Diese Kartenleser stellen nur die Verbindung zur Chipkarte her.
- **Klasse 2:** Hier bietet der Kartenleser neben der Kontaktiereinheit zur Chipkarte auch eine Tastatur zur Eingabe der PIN.
- **Klasse 3:** Solche Leser haben die Kontaktiereinheit, eine Tastatur zur PIN-Eingabe und eine kleine Anzeige für zu signierende Daten

<sup>9</sup> Es wird nicht das gesamte zu signierende Dokument an die Chipkarte übermittelt, sondern ein so genannter Hash-Wert als Repräsentant des Dokuments. Der Hash-Wert oder ein Teil des Hash-Werts werden in Software errechnet.

<sup>10</sup> Home-Banking Computer Interface (HBCI) ist eine vom deutschen Zentralen Kreditausschusses (ZKA) beschlossene Spezifikation.

- Klasse 4 Leser haben zusätzlich ein weiteres sicheres Chip-Modul integriert, um die Authentifizierung des Lesers gegenüber der Chipkarte des Kunden zu ermöglichen.

Für den allgemeinen Fall qualifizierter Signaturen genereller Daten sind nur die ersten beiden Klassen 1 und 2 praktisch relevant<sup>11</sup>. Es wird deshalb in Folge nur zwischen Kartenlesern mit PIN-Pad (das heißt Klasse 2 oder höher mit Tastatur am Kartenleser) und solchen ohne PIN-Pad (das heißt Klasse 1) unterschieden.

Kartenleser ohne PIN-Pad sind zunehmend verbreitet oder oft schon in PCs und Laptops integriert. Auch dass Kartenleser mit PIN-Pad zur Eingabe der PIN am Leser spezielle Treiber benötigen, die in Standard-Betriebssystemen oft nicht „Plug&Play“ installierbar sind, erschwert die Verwendung in allgemeiner breiter Anwendung<sup>12</sup>. Es wird deshalb in Folge das realistische Risiko der Verwendung eines Kartenlesers ohne PIN-Pad eingeschätzt.

## 4. Angriffsmöglichkeiten

### 4.1. Theoretische Angriffsszenarien

Auf Basis des zuvor eingeführten Schemas bieten sich verschiedenen Angriffspunkte.

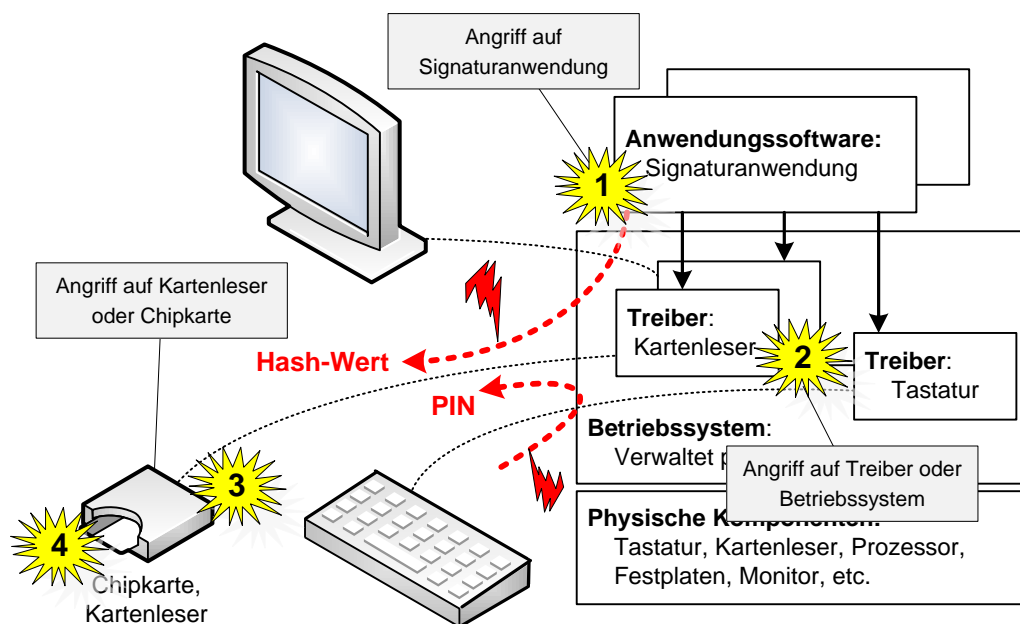


Abbildung 2: Angriffspunkte auf das System Software – Treiber– Karte – Leser

Wie in Abbildung 2 skizziert ist, sind im Wesentlichen vier Angriffspunkte zu betrachten:

1. Ein Kompromittieren der Signatursoftware würde ein Verändern der Anzeige der zu signierenden Daten, der Aufbereitung dieser Daten (Bilden des Hash-Wertes), der Übermittlung an den Treiber oder, sofern von der Signatursoftware gestellt, der PIN-Eingabe erlauben.
2. Ein Angriff auf Funktionen des Betriebssystems oder der Kartenleser-Treiber Software kann die Kommunikation mit dem Kartenleser und damit mit der Chipkarte

<sup>11</sup> Klasse 3 Leser werden mit ihrer beschränkten Anzeigemöglichkeit vor allem in speziellen Anwendungen verwendet, wo der Umfang der zu signierenden Daten beschränkt ist, etwa Betrag und Kontonummer in Online-Überweisungen. Anwendungsbeispiele für Klasse 4 Leser sind Point-of-Sales Terminals.

<sup>12</sup> Im PC-Umfeld sind die Standards PC/SC und CT-API verbreitet. PC/SC wird von Microsoft Systemen standardmäßig unterstützt und meist automatisch installiert. Die PIN-Eingabe am Kartenleser wird in Version 2.0 von PC/SC unterstützt, jedoch setzen dies noch nicht alle Treiber oder Anwendungen um. PIN-Eingabe am Kartenleser wird bei CT-API unterstützt, dazu ist aber eine gesonderte Installation z.B. über CD des Herstellers notwendig.

kompromittieren. Damit können der Hash-Wert ersetzt oder, wieder sofern in Software umgesetzt, die PIN gelesen werden.

3. Eine Manipulation des Kartenlesers oder seiner Verbindungen erlaubt ein Auslesen von PIN oder Verändern des Hash-Wertes.
4. Der letzte Angriffspunkt wäre die Chipkarte selbst.

Ein Kompromittieren des Kartenlesers selbst (3.) bedarf im Allgemeinen einer physikalischen Manipulation. Für den Einsatz im privaten Heimbereich des Signators oder im kontrollierten Arbeitsumfeld wird man von derartigen Eingriffen nicht ausgehen. Auch ein Brechen der Chipkarte (4.) kann durch die hohen Sicherheitsstandards als kaum praktikabel ausgeschlossen werden. Es werden deshalb nur die Manipulationen der Signatursoftware und von Funktionen des Betriebssystems weiter betrachtet.

#### **4.2. Praktische Relevanz**

Beide betrachtete Angriffsszenarien sind dann relevant, wenn ein Angreifer die Kontrolle über den Rechner mit entsprechenden Rechten, etwa mit Administrator-Rechten hat. In diesem Fall ist eine Manipulation von Softwareelementen immer denkbar. Es ist erst dann von sicherheitsrelevanten Beeinträchtigungen der Signaturumgebung, die sich aus der Wahl des Kartenlesers ergeben, auszugehen, wenn das System des Signators durch den Angreifer bereits kompromittiert ist. Schadsoftware (Malware) kann unterschiedlicher Ausprägung sein, einige davon sind in Folge gelistet:

- Trojanische Pferde, die Signatoren in das System einbringen.
- Viren oder Würmer mit spezifischen Angriffsroutinen.
- Client-seitiges cross-site scripting, die Schwachstellen installierter Software ausnutzen.
- Spyware oder Keylogger, die Passworte oder PINs ausspionieren..

Derartige Schadsoftware ist weit verbreitet. Wenngleich keine konkreten ausgenutzten und breit umgesetzten Angriffe auf Signaturlösungen bekannt sind, sind solche bei kompromittierten Systemen denkbar und zu betrachten. Insbesondere, als im akademischen Umfeld in den letzten Jahren mehrmals Möglichkeiten veröffentlicht oder demonstriert wurden, die Signaturumgebung zu beeinträchtigen. Dies ist nicht verwunderlich, als es bei PCs mit aktuellen Betriebssystemen grundsätzlich nicht möglich ist, eine Manipulation von Software zu verhindern<sup>13</sup>, sobald ein Angreifer die Kontrolle über das System als Administrator übernommen hat.

#### **4.3. Kartenleser vs. Angriffsmöglichkeiten**

Wenngleich Schadsoftware wie für den Identitätsdiebstahl oder das Ausspionieren von Passwörtern für Online-Anwendungen weit verbreitet sind, ist das Risiko für die elektronische Signatur etwas zu relativieren. Einerseits muss zum Zeitpunkt des Angriffes die Karte gesteckt sein und der Angreifer kann nicht wie bei abgefangenen Passwörtern vom System des Signators unabhängig Angriffe starten, andererseits bedarf es immer zweier Angriffsroutinen:

- Es muss die Auslösefunktion für eine Signatur gestartet werden (der PIN abgefangen und an die Chipkarte übermittelt werden).
- Es müssen zu signierende Daten generiert oder modifiziert und an die Chipkarte gegeben werden.

Werden Kartenleser mit PIN-Pad verwendet, so ist der erste Fall dadurch abgedeckt, dass der PIN vom Signator direkt am PIN-Pad eingegeben wird und vom Angreifer nicht ausgelesen werden kann. In der Standardinstallation werden aber oft auch PC/SC Treiber mit-installiert, die die direkte Übergabe des PINs ohne Eingabe des Lesers ermöglichen<sup>14</sup>. Der Signator kann damit jeglichen Sicherheitsgewinn eines Kartenleser mit PIN-Pad dadurch verlieren,

---

<sup>13</sup> Es werden hier Ansätze wie Trusted Computing und Trusted Platform Modules (TPM) nicht betrachtet. Dabei handelt es sich auch um hardware-gestützte Sicherheit.

<sup>14</sup> Es gibt auch Klasse 2 Leser am Markt, die die Übermittlung der PIN über Abfangen von Chipkartenbefehlen verhindern und die Eingabe an der Tastatur des Kartenlesers erzwingen.

dass er einmal die PIN nicht am Kartenleser, sondern in einer Art Phishing-Angriff über die Software-Eingabemöglichkeit eingibt, was dem Angreifer das Ausspionieren dieser und die Übermittlung über den alternativen Treiber ermöglicht, der den Kartenleser mit PIN-Pad wie einen ohne PIN-Pad anspricht.

In jedem Fall, unabhängig davon, ob der Kartenleser ein PIN-Pad hat, oder nicht, ist ein Angriff auf die elektronische Signatur nur dann sinnvoll, wenn die zu signierenden Daten manipuliert oder vom Angreifer eigene zu signierende Daten generiert werden. Ein Keylogger alleine, wie er etwa zum Abfangen von Passwörtern in Online-Anwendungen verwendet wird, ist zwar denkbar, um bei Kartenlesern ohne PIN-Pad eine PIN abzufangen. Der Angreifer benötigt aber immer auch eine zweite Angriffsroutine zur Modifikation oder Erstellung zu signierender Daten<sup>15</sup>.

## 5. Schlussfolgerungen

Nimmt man die Analyse der Angriffsmöglichkeiten und berücksichtigt die gesetzliche Situation, so lassen sich für die Auswahl eines Kartenlesers folgende Schlussfolgerungen ziehen:

1. Kartenleser ohne PIN-Pad sind Stand der Technik und sind in zunehmendem Umfang in Geräten vorzufinden. Microsoft setzt auch generell auf die PC/SC Schnittstelle und hat damit derartige Leser in breiter Form in das System integriert.
2. Im internationalen Umfeld sind derartige Kartenleser anerkannt und können auch für die qualifizierte Signatur verwendet werden. Damit ist aus der EU Signaturrechtlinie kein Hinderungsgrund abzuleiten, Kartenleser ohne PIN-Pad zu verwenden.
3. Die Österreichische Gesetzeslage verordnet eine gewisse Sicherheit für alle im Zusammenhang mit der qualifizierten Signatur verwendeten Elemente (Hard- und Software) und schützt damit den Signator und den ZDA vor willkürlichen und zufälligen Fehlsituationen. Dieser Schutz wurde auch in der Gesetzeslage ab 2008 beibehalten. In Analogie zu den Sicheren Signaturerstellungseinheiten kann dieser Schutz eine Kombination aus technischen und organisatorischen Maßnahmen sein.
4. Wie bei allen Umgebungen, die für die qualifizierte Signatur eingesetzt werden, ist davon auszugehen, dass der Benutzer Maßnahmen trifft, dass er auch das System und die Umgebung unter seiner vollen Kontrolle hat. Daher ist seitens des Signators sicherzustellen, dass das Gerät frei von Viren und Schadsoftware ist.
5. Im Falle von Kartenlesern ohne PIN-Pad ist die Schadsoftwareklasse der Keylogger in besonderer Weise zu betrachten. Auch wenn diese allein nur den PIN ausspähen und damit eine beachtliche Gefahr darstellen, benötigen Sie noch eine zweite Schadsoftwarekomponente, die ein "falsches Dokument" oder zumindest einen falschen Hashcode unterschleibt. Diese zweite Komponente ist in Kombination mit einer modifizierten Anzeige auch bei Kartenlesern mit PIN-Pad in der Lage, die Signatur beliebig zu kompromittieren, sodass das Augenmerk auch auf diese zweite Komponente generell zu legen ist.
6. Generell sind die gleichen Mechanismen seitens des Signators einzusetzen, um beide genannten Schadkomponenten auszuschalten und es sind diese daher generell seitens des ZDA zu "empfehlen".
7. Auch wenn aus der allgemeinen Empfindung dies unterschiedlich wahrgenommen wird, ist das Sicherheitsrisiko in einer Umgebung, die der Benutzer kontrolliert (z.B. privater PC), in einer vergleichbaren Größenordnung. Diesem Umstand wird auch in den neuen Systemen z.B. Vista und Trusted Computing Rechnung getragen.

---

<sup>15</sup> Im Beispiel E-Government Anwendung mit der Bürgerkarte umfasst dies für den erfolgreichen Angriff nicht nur das Auslösen einer Signatur, sondern auch die Abarbeitung des Anmeldeprotokolls.

Als Schlussfolgerung kann gesehen werden, dass die Sicherheitsmaßnahmen, die notwendig sind, um eine Signaturumgebung mit Kartenleser ohne PIN-Pad zu betreiben, auch in Systemen mit PIN-Pad gesetzt werden müssen.


## 6. Handlungsempfehlungen

Um auch Chipkartenleser ohne PIN-Pad sicher betreiben zu können, muss der Signator das System frei von Schadsoftware halten bzw. die Möglichkeiten, dass Angreifer solche Schadkomponenten einspielen, minimieren.

Empfohlenen Vorkehrungen beim Einsatz von Kartenlesern ohne PIN-Pad sind:

1. Aktualisieren Sie Ihr Betriebssystem und Ihre Software regelmäßig. Spielen Sie insbesondere sicherheitsrelevante Updates und Patches immer ein<sup>16</sup>. Damit werden Angriffspunkte über bekannte Fehler – so genannte Exploits – vermieden.
2. Verwenden Sie einen aktuellen Virens scanner<sup>17</sup> und lassen Sie diesen die Virensignaturen laufend automatisch aktualisieren<sup>18</sup>. Damit sollen Schadkomponenten erkannt werden.
3. Nutzen Sie eine Personal Firewall bzw. wo möglich auch eine Netzwerk-Firewall<sup>19</sup>. Dies vermeidet Angriffe aus dem Internet auf Ihr System.
4. Installieren Sie nur Software aus vertrauenswürdigen Quellen. Öffnen Sie keine Email-Anhänge von unbekanntem Absendern oder installieren Sie keine Software unbekannter Herkunft aus dem Internet.
5. Verwenden Sie im täglichen Betrieb nur Benutzerkonten mit eingeschränkten Rechten und verwenden Sie das Administratorenkonto nur wenn notwendig, etwa für Installationen. Damit sind die Möglichkeiten eines Angreifers, dass Schadsoftware kritische Funktionen der Treiber und des Betriebssystems kompromittiert, deutlich eingeschränkt.
6. Stecken Sie die Chipkarte nur für den Signaturvorgang und lassen Sie die Karte nicht im Chipkartenleser stecken.

Die Empfehlungen sind allgemein für sicherheitsrelevante Anwendungen zu sehen und ergeben (bis auf 6.) keine spezifischen Ausprägungen für die Verwendung von Chipkarten und der Art des Chipkartenlesers. Dies da mit Chipkartenlesern ohne PIN-Pad in nicht kompromittierten Umgebungen kein erhöhtes Risiko zu Lesern mit PIN-Pad einhergeht. Ist ein System jedoch gebrochen, dann kann auch bei Lesern mit PIN-Pad nicht mehr davon ausgegangen werden, dass die Signaturumgebung nicht beeinträchtigt ist.


Signaturwert	GHIPZx6T8srNw/MgO7G41Hd6mJlKJI5KE59webRWLYwjef9kx3rTtmIarZziQiBp	
	Unterzeichner	Prof. Dr. Reinhard Posch, Wissenschaftlicher Gesamtleiter
	Datum/Zeit-UTC	2008-01-29T22:13:59Z
	Aussteller-Zertifikat	CN=a-sign-Premium-Sig-02,OU=a-sign-Premium-Sig-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	65090
	Methode	urn:pdfsigfilter:bka.gv.at:text:vl.1.0
	Parameter	etsi-bka-1.0@1201644839-101999756@32295-11138-0-29115-24768
Prüfhinweis	Prüfservice: <a href="http://demo.a-sit.at/el_signatur/verification">http://demo.a-sit.at/el_signatur/verification</a>	

<sup>16</sup> z.B. kritische Updates bei Windows

<sup>17</sup> Moderne Virens scanner haben meist weitere sinnvolle Sicherheitsfunktionen wie Phishing-Filter, Anti-Spyware Funktionen, etc.

<sup>18</sup> Virens scanner haben meist Default-Einstellungen, die an die Aktualisierungsfrequenz der Hersteller sinnvoll angepasst sind.

<sup>19</sup> Internet-Router / WLAN Router haben meist auch Firewall-Funktionalität

Signaturwert	1vNw4yRFP0hvMXtNPgc69FYnB3l8DvpKzaRpCXfYTU8YKZDMYnXSzBhFirkLkMO7	
	Unterzeichner	Geschäftsführender Vorstand, Manfred Holzbach
	Datum/Zeit-UTC	2008-01-31T09:35:31Z
	Aussteller-Zertifikat	CN=a-sign-Premium-Sig-02,OU=a-sign-Premium-Sig-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	97349
	Methode	urn:pdfsigfilter:bka.gv.at:text:v1.1.0
	Parameter	etsi-bka-1.0@1201772132-1816671@31007-29021-0-23034-5142
Prüfhinweis	Informationen zur Signaturprüfung finden Sie unter: <a href="http://www.a-sit.at/de/dokumente_publicationen/a-sit_signaturen/index.php">www.a-sit.at/de/dokumente_publicationen/a-sit_signaturen/index.php</a> .	