# Masterarbeit

## Geldspielgeräte und die SpielV

Eine Betrachtung der technischen Umsetzung einer politischen Vorgabe unter den Aspekten „Sicherheit“ und „Stand der Technik“

Autor:
Thomas Noone
Am Köllenholz 19
86637 Wertingen-Hirschbach

**Sommersemester 2008**
**Fakultät für Informatik**
**Hochschule Augsburg**
**Professor Burkhard Stork**

**Abstract**

Die Physikalisch-Technische Bundesanstalt PTB definiert das in § 7 SpielV geforderte Prüfverfahren so, dass Geldspielautomaten alle 24 Monate durch öffentlich bestellte und vereidigte Sachverständige oder von der PTB zugelassene Stellen zu unterziehen sind. Hierfür wurde ein neuer Bestellungstenor durch die Industrie- und Handelskammern geschaffen. Mit Bestellung der ersten Sachverständigen, die bereits zuvor für Informationstechnik öffentlich bestellt waren, ergaben sich jedoch Zweifel an der grundsätzlichen Aussagekraft des definierten Prüfverfahrens. Denn moderne Geldspielgeräte sind zumeist PCs mit handelsüblichen Betriebssystemen und proprietärer Software, werden jedoch nicht als Gesamtsystem geprüft. Diese Masterarbeit befasst sich mit dem bestehenden Prüfverfahren und der hierfür als Basis dienenden Bauartzulassung der PTB, analysiert anhand eines Risk Assessment diejenigen Sicherheitsaspekte, die ein Zulassungs- und Prüfverfahren tatsächlich berücksichtigen sollte und stellt diese dem bestehenden Verfahren gegenüber. Es wird ein alternatives Zulassungs- und Prüfverfahren entworfen und mit dem bestehenden Verfahren verglichen. Abschließend werden die Möglichkeiten einer schrittweisen Verbesserung des bestehenden Ist-Verfahrens und deren Aussicht auf eine Umsetzung erörtert.

**Erstellungserklärung**

Ich erkläre hiermit, diese Arbeit selbständig verfasst und noch nicht anderweitig für Prüfungszwecke vorgelegt zu haben.

Es wurden keine anderen als die angegebenen Quellen und Hilfsmittel benutzt.

Wörtliche und sinngemäße Zitate sind als solche gekennzeichnet.

Wertingen, den 24.06.2008

Thomas Noone

# Inhalt

## i. Abbildungsverzeichnis

## ii. Tabellenverzeichnis

# 1 Einleitung

Der Autor ist öffentlich bestellter und vereidigter Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung. Während des zweiten Semesters des „Master of Science“-Studienganges hat er sich zusätzlich mit der öffentlichen Bestellung für die Überprüfung von Geldspielgeräten befasst.

Da aus technischer Sicht betrachtet Geldspielautomaten ein klassisches IT-Sicherheitsrisiko darstellen - denn es handelt sich im Grunde um Computer, die auch als Teil eines Client-Server-Systems eingesetzt werden können, boten sich diese als Gegenstand einer Risikoanalyse an.

Im weiteren Verlauf des Studiums und während der parallel erfolgenden Vorbereitungen auf die Bestellung ergaben sich weitergehende Aspekte für den Autor, die ein Ausweiten dieser Arbeit auf die Arbeitsweise der Zulassungsbehörde PTB (Physikalisch-Technische Bundesanstalt) sinnvoll erscheinen ließ: Zum einen gab es Ungereimtheiten in deren Zulassungspraktiken, zum anderen war dieselbe Fachabteilung der PTB bereits wegen ihrer Zulassungspraktiken für die Wahlcomputer in die Kritik geraten [ct1].

Diese Arbeit bedient sich der im Aufbaustudiengang „Master of Science“ der Hochschule Augsburg gelehrten Verfahren zu u.a. Kryptografie, Secure Software Engineering, Softwarearchitektur, Kommunikation und kooperative Systeme und Performance Evaluation, um die Sicherheitsrisiken zu analysieren und sichere Alternativen aufzuzeigen. Da dies eine Änderung des analysierten Zulassungs- und Prüfverfahrens zwingend erforderlich machen würde, wird die praktische Umsetzung einer sicheren Lösung erörtert.

Diese Arbeit wurde bereits frühzeitig in einer ersten Rohfassung mit Risikoanalyse an Professor Stork übersandt. Damit ist auch dokumentiert, dass die Risikoanalyse bereits fertiggestellt war, bevor es zu den in dieser Arbeit genannten Vorfällen kam, welche eine nachträgliche Beurteilung der Risikoanalyse erlauben.

## 1.1 Umfang der Arbeit

Diese Arbeit betrachtet zunächst den Markt für Geldspielgeräte im Allgemeinen und befasst sich dabei auch mit den vorherrschenden Markstrukturen.

Anschließend werden beispielhaft einige Elemente im Prozess der Gerätebauartzulassung durch die PTB analysiert, bei denen grundsätzliche Fehler in der technischen Umsetzung vorliegen, womit der gesamte Zulassungsprozess einer Gerätebauart in Frage zu stellen ist.

Der darauf aufbauende Überprüfungsprozess der PTB für die am Markt befindlichen Geldspielgeräte wird einer Risikoanalyse unterzogen und die Unsicherheitsfaktoren im Prozessablauf dokumentiert.

Anhand eines verbesserten Soll-Prozesses wird demonstriert, wie eine sichere Überprüfung nach dem geforderten Stand der Technik aussehen müsste. Dieser Prozess wird zunächst detailliert entworfen und anschließend optimiert.

Danach wird der vorgestellte Soll-Prozess der aktuell gängigen Praxis gegenübergestellt. Es wird erklärt, welche Schritte im Einzelnen nötig wären, um den fehlerhaften Ist-Prozess schrittweise gegen einen sicheren Soll-Prozess zu ersetzen. Dabei werden praktische Beispiele erörtert, die zeigen, wie und warum das Verhalten einzelner Parteien einer Umsetzung im Wege steht, und dieses wird dann in Bezug zur erfolgten Risikoanalyse gesetzt.

## 1.2 Abgrenzungen

Diese Arbeit befasst sich weder damit, welche Absicht der Gesetzgeber mit der Spielverordnung SpielV verfolgt, noch mit den Motiven für die erfolgte Umsetzung durch die PTB.

Es wird auch nicht weiter berücksichtigt, inwieweit alternative Vorgehensweisen rechtlich notwendig bzw. zulässig sind.

# 2 Motivation

Die gutachterliche Tätigkeit auf dem Gebiet der Informationssysteme erfordert eine neutrale, nachvollziehbare und nachprüfbare Argumentation zu getroffenen Feststellungen, wie auch in der Sachverständigenordnung festgeschrieben [svo1].

Diese schien dem Autor (und weiteren Sachverständigenkollegen) bei der Überprüfung von Geldspielgeräten nicht gegeben.

Für die Bauartzulassung [spielv1] ist die Physikalisch-Technische Bundesanstalt (PTB) zuständig, und zwar der Fachbereich 8.5 „Metrologische Informationstechnik“ [ptb3].

Da es sich hierbei um denselben Fachbereich handelt, der für die Zulassung von „Software und elektronische Wahlen“ zuständig ist, sah der Autor den potenziellen Zusatznutzen für Dritte, mit dieser Arbeit eine grundsätzliche Vergleichsbasis zwischen der Handhabung von Geldspielgeräten und Wahlcomputern durch die PTB herstellen zu können.

## 2.1 Verordnung über Spielgeräte und andere Spiele mit Gewinnmöglichkeit (Spielverordnung - SpielV)

Mit Inkrafttreten der SpielV erhielten im März 2006 die ersten Geräte eine Bauartzulassung durch die Physikalisch-Technische Bundesanstalt (PTB). Folglich sind ab März 2008 laut § 7 SpielV Prüfungen durchzuführen:

*SpielV § 7 Aus-dem-Verkehr-Ziehen von Spielgeräten*

*(1) Der Aufsteller hat ein Geldspielgerät spätestens 24 Monate nach dem im Zulassungszeichen angegebenen Beginn der Aufstellung und danach spätestens alle weiteren 24 Monate auf seine Übereinstimmung mit der zugelassenen Bauart durch einen vereidigten und öffentlich bestellten Sachverständigen oder eine von der Physikalisch-Technischen Bundesanstalt zugelassene Stelle auf seine Kosten überprüfen zu lassen.*

*(2) Wird die Übereinstimmung festgestellt, hat der Prüfer dies mit einer Prüfplakette, deren Form von der Physikalisch-Technischen Bundesanstalt festgelegt wird, am Gerät sowie mit einer Prüfbescheinigung, die dem Geräteinhaber ausgehändigt wird, zu bestätigen.*

*(3) Der Aufsteller darf ein Geldspielgerät nur aufstellen, wenn der im Zulassungszeichen angegebene Beginn der Aufstellung oder die Ausstellung einer nach Absatz 2 erteilten Prüfplakette nicht länger als 24 Monate zurückliegt.*

*(4) Der Aufsteller hat ein Geld- oder Warenspielgerät, das in seiner ordnungsgemäßen Funktion gestört ist, dessen Spiel- und Gewinnplan nicht leicht zugänglich ist, dessen Frist gemäß Absatz 3 oder dessen im Zulassungszeichen angegebene Aufstelldauer abgelaufen ist, unverzüglich aus dem Verkehr zu ziehen.*

## 2.2 Die Überprüfung

Der Gesetzestext enthält keine Vorgaben darüber, wie die Überprüfung stattfinden muss, nur dass dabei die „Übereinstimmung mit der zugelassenen Bauart“ zu überprüfen ist.

Von der PTB wird eine Checkliste vorgegeben, basierend auf dem Dokument „Gegenstand der Geräteüberprüfungen“ [ptb1]. Die Überprüfung beinhaltet zum einen eine Sichtprüfung auf

Konformität von äußerlichen Merkmalen nach Vorgaben der PTB, mit der Überprüfung von Tastenfunktionen und der am Display abrufbaren Gerätedaten.

Zum anderen ist im Geräteinneren entweder über eine serielle Schnittstelle eine ausführbare Datei abzurufen oder nach Abziehen von EPROMs diese auszulesen. Mittels des CRC32-Algorithmus ist eine Prüfsumme davon zu bilden. Diese hat mit einer von der PTB vorgegebenen Prüfsumme identisch zu sein, die für alle Geräte dieser Bauartzulassung gilt. Für die Überprüfung muss laut PTB „bedenkenlos“ eine von Automatenherstellern entwickelte Software benutzt werden.

Sind die Prüfsummen identisch und ergibt sich anhand der Sichtprüfung kein Grund zur Beanstandung, darf laut PTB die Prüfplakette vergeben werden.

## 2.3 Öffentlich bestellte und vereidigte Sachverständige für Systeme und Anwendungen bzw. Technik und Systeme der Informationsverarbeitung

§ 7 (1) SpielV schreibt ausdrücklich vereidigte und öffentlich bestellte Sachverständige oder von der PTB zugelassene Stellen als Prüfer vor.

In der Regel werden öffentlich bestellte und vereidigte Sachverständige von Industrie- und Handelskammern bestellt, nachdem sie ein aufwändiges Prüfungsverfahren durchlaufen haben und abschließend von einer Prüfungskommission aus Sachverständigen schriftlich und mündlich geprüft wurden. Das gesamte Bestellungsverfahren dauert ohne weiteres 12 Monate oder länger.

Im Falle des Sachgebiets 530 („Überprüfung von Geldspielgeräten“) wird für Antragsteller auf eine öffentliche Bestellung eine Sachkundeprüfung durch die IHKs durchgeführt mit anschließender praktischer Prüfung durch die PTB.

Alternativ kann die PTB z. B. Mitarbeiter des TÜV Rheinland derselben praktischen Prüfung unterziehen. Nach Bestehen der Prüfung darf diese Person für diese zugelassene Stelle dieselbe Überprüfung vornehmen wie öffentlich bestellte und vereidigte Sachverständige für die Überprüfung von Geldspielgeräten.

Aufgrund der thematischen Nähe haben die IHKs auch Sachverständige für Systeme und Anwendungen der Informationsverarbeitung bzw. Technik und Systeme der Informationsverarbeitung vorgeschlagen, sich für das Sachgebiet 530 bestellen zu lassen. Hierbei erfolgt lediglich die praktische Prüfung durch die PTB.

## 2.4 Erste Ungereimtheiten

Die von der PTB vorgegebene Vorgehensweise zur Überprüfung von Geldspielgeräten reflektiert nicht die von Sachverständigen für Informationssysteme verlangte und praktizierte Sorgfalt.

- Das Auslesen einer Datei oder eines Speicherinhalts in der beschriebenen Form lässt keine Aussage darüber zu, ob die Inhalte auch mit den Programmen übereinstimmen, die in einem Gerät tatsächlich laufen.
- Die Überprüfung mit Hilfe einer vom Gerätehersteller gelieferten Software ist ohne Verifikation deren Unbedenklichkeit nicht sicher.

- Die Überprüfung anhand einer CRC32-Prüfsumme ist ebenfalls bedenklich, da dieser Algorithmus nicht einmal eine Aussage zur Integrität der geprüften Daten erlaubt, geschweige denn die Sicherheit eines üblichen kryptografischen Verfahrens bietet.

- Die Prüfkonfigurationen, die der Bauartprüfung der PTB zugrunde liegen, erlauben keine aussagekräftigen Messungen [ptb2].

Im Rahmen von Herstellerschulungen und Werksbesichtigungen ergaben sich noch weitere Aspekte:

- Neuere Geräte sind im Grunde herkömmliche Industrie-PCs, teils mit Windows XP als Betriebssystem.

- Die Geräte besitzen LAN-Schnittstellen zur Kommunikation mit zentralen Servern und sind somit als klassische Clients einzustufen.

- Schnittstellen für Kartenleser zur Abfrage einer Betriebserlaubnis-PIN konnten nachweislich in der Vergangenheit zur Manipulation des Spielverhaltens verwendet werden, womit Hard- und Softwareschnittstellen für mehr als nur den zugelassenen Spielbetrieb ausgelegt sein könnten [uadv1].

## 2.5 Zusammenfassung Motivation

Die auf den ersten Blick offensichtlichen Schwächen der von der PTB vorgegebenen Konformitätsprüfung bezüglich Nachweisbarkeit der Ergebnisse und Überprüfbarkeit im Allgemeinen ließen grundsätzliche Probleme im gesamten Zulassungs- und Prüfverfahren erwarten.

Dies schien dem Autor eine ideale Ausgangsbasis, um die im Masterstudium vermittelten Grundlagen praxisnah einzusetzen.

# 3 Der Markt

Laut der „AWI Automaten-Wirtschaftsverbände-Info GmbH“ umfasste der deutsche Markt für Geldspielgeräte im Jahre 2006 ca. 220.000 Geld-Gewinn-Spiel-Geräte und sorgte für 52.000 Arbeitsplätze bei den Aufstellunternehmern und 10.000 Arbeitsplätze in Großhandel und Industrie, mit davon mehr als 75 % weiblichen Mitarbeitern. 6.000 hochtechnisierte Betriebe erzeugen, verteilen oder betreiben Unterhaltungsspiele in Deutschland [awi01]. Die jährlichen Euro-Umsätze bewegen sich im einstelligen Milliardenbereich.

## 3.1 Die Hersteller

Das sogenannte „kleine“ Glücksspiel (im Gegensatz zum „großen“ Glückspiel wie etwa Lotto oder Roulette) wird in Deutschland von drei Herstellern von Geldspielgeräten dominiert:

- adp Gauselmann GmbH (adp)
- NSM-Löwen Entertainment GmbH (NSM)
- Bally-Wulff Entertainment GmbH (Bally-Wulff)

Zwar gibt es noch einige kleine Hersteller am Markt, aber aufgrund der vorherrschenden Markt- und Gesetzeslage haben sich z. B. große Hersteller des asiatischen Marktes in Deutschland bisher nicht etablieren können.

Die Hersteller verkaufen ihre Geräte sowohl direkt an Aufsteller wie auch an Händler. Gleichzeitig betreiben die großen Hersteller eigene Spielhallenketten, womit sie im direkten Wettbewerb zu ihren Abnehmern stehen.

In den letzten Jahren haben sich Geschäftsmodelle durchgesetzt, bei denen „gut laufende“ Geräte nur noch geleast werden können. Praktisch alle neueren Geräte verfügen über Netzwerkschnittstellen, die teilweise mit zentralen Hersteller-Servern vernetzt sind.

Paul Gauselmann von adp wurde 1993 das Bundesverdienstkreuz verliehen [adp4], Karl Besse, Präsident des Bundesverbandes Automatenunternehmer e.V. (BA) wurde 2008 von Bundespräsident Horst Köhler mit der Verdienstmedaille der Bundesrepublik Deutschland ausgezeichnet [bes1], womit man der Branche auch gute Kontakte zur Politik unterstellen darf.

## 3.2 Die Händler

Die Händler stehen teilweise im direkten Wettbewerb zu den Herstellern, da Hersteller zum einen die Aufsteller direkt bedienen, zum anderen die herstellereigenen Ketten, die sowohl Aufsteller wie Händler umgehen bzw. mit diesen im Wettbewerb stehen. Händler werden in dieser Arbeit nicht näher betrachtet, da sie lediglich eine Zwischenstation für den Verkauf der Geräte vom Hersteller an den Aufsteller darstellen, durch Leasing- bzw. Mietmodelle oft außen vor bleiben und im aufgezeigten Ist-Prozess keine Rolle spielen.

## 3.3 Die Aufsteller

Bei den Aufstellern (und herstellereigenen Spielhallen) befinden sich die meisten der 52.000 Arbeitsplätze. Aufsteller sind durch die Leasing-Konzepte und die Gerätevernetzung mit passendem Dienstleistungsangebot der Hersteller in den letzten Jahren immer stärker in deren Abhängigkeit geraten und stehen dazu noch im Wettbewerb zu den herstellereigenen Spielhallen.

### 3.4 Die Spieler

Nach Lektüre der öffentlich zugänglichen „Technischen Richtlinie – Zur Sicherung der Prüfbarkeit und Durchführung der Bauartprüfung von Geldspielgeräten im Sinne von § 33c Gewerbeordnung“ [ptb2] ist eindeutig geklärt, dass Geldspielgeräte nur dahingehend in ihrem Verhalten vorhersehbar sein müssen, dass sie sich an die Vorgaben des § 7 SpielV halten.

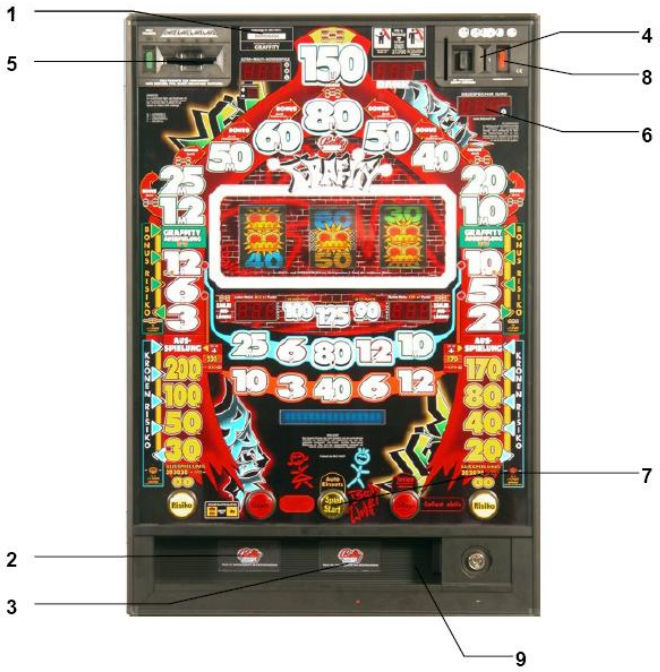
Diese Vorgaben erlauben beispielsweise einen Kasseninhalt (Rohertrag) von maximal € 33,-- pro Stunde für den Aufsteller, wobei der Aufsteller seine „Quote“ in einem bestimmten Maße einstellen kann. Pro Stunde darf für den Spieler der maximale Verlust € 80,-- und der maximale Gewinn € 500,-- betragen.

Zwar gibt es den Personenkreis, der nur zum Spaß mal eine Münze einwirft und sich über einen möglichen Gewinn freut, der Kunde ist jedoch in der Regel mehr oder weniger spielsüchtig und entweder mit der technischen Richtlinie nicht vertraut oder nach anderen Kriterien beurteilend.

Tatsächlich werden „gut laufende“ Geräte (Geräte, welche die Spieler als gewinnbringend wahrnehmen) von Spielern detailliert beobachtet, sodass sich beispielsweise eine Geräteüberprüfung, bei der das Gerät geöffnet und ein PC angesteckt werden muss, vor den Augen der Kunden von selbst verbietet. Ebenso sind Zahltage (oder die Tage kurz davor) kein wirklich guter Zeitpunkt, um Geräte zu prüfen, da sie Zweifel bei den Spielern bezüglich ihrer erhofften Gewinnaussichten hervorrufen.

## 4 Kurzüberblick Geldspielgeräte

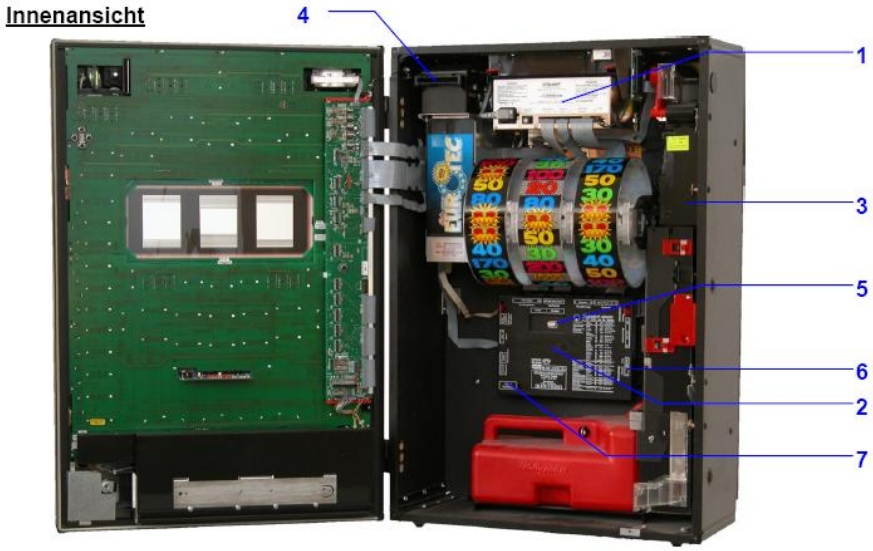
Die folgenden Bilder zeigen Außen- und Innenansicht aus dem Zulassungsschein eines „Bally-Wulff GRAFFITY“-Geldspielgeräts [ptb4]:




**Funktionselemente:**

1. Gerätekennzeichnungsfeld
2. Zulassungszeichen-Fach
3. Vorgesehener Platz für Nachprüf-Plakette
4. Münzeinwurf mit Auswurftaste bei Versagen
5. Banknotenannahme
6. Geldverfügungsspeicher
7. Umschalttaste für Spiele mit automatischer bzw. Einzel- Einsatzabbuchung und Auslösetaste für Einzel- Einsatzabbuchung
8. Auszahlungstaste für Geldverfügungsspeicher
9. Münzausgabe-Fach

Bild 1: Außenansicht




**Bauteile / -gruppen:**

1. Netzteil
2. Steuerungsprogramm- Einheit
3. Münzeinheit
4. Banknotenannahme
5. Schnittstelle (a)
6. Schnittstelle (b)
7. Schnittstelle (c)

Bild 2: Innenansicht

Hinter der schwarzen Plastikblende (Bild 2, 2.) befinden sich bei diesem Modell zwei EPROMs mit dem per EPROM-Lesegerät auszulesenden Binärcode. Kommt man dabei auf dieselben CRC32-Prüfsummen wie in der Zulassung notiert, so wird dies von der PTB als Nachweis dafür betrachtet, dass der Binärcode der EPROMs bitweise identisch ist zu dem ursprünglich bei der PTB hinterlegten Binärcode zum Zeitpunkt der Bauartprüfung. Der Binärcode anderer Geräte, z. B. von adp, kann auch nur über eine serielle Schnittstelle auslesbar sein, welche jedoch Software des jeweiligen Herstellers zum Auslesen der Daten verlangt.

Alle Geldspielgeräte sollen zwei logische Komponenten, die „Spielsteuerung“ und die „Kontrolleinrichtung“, aufweisen. Diese werden durch den Hersteller in Soft- oder Hardware implementiert.

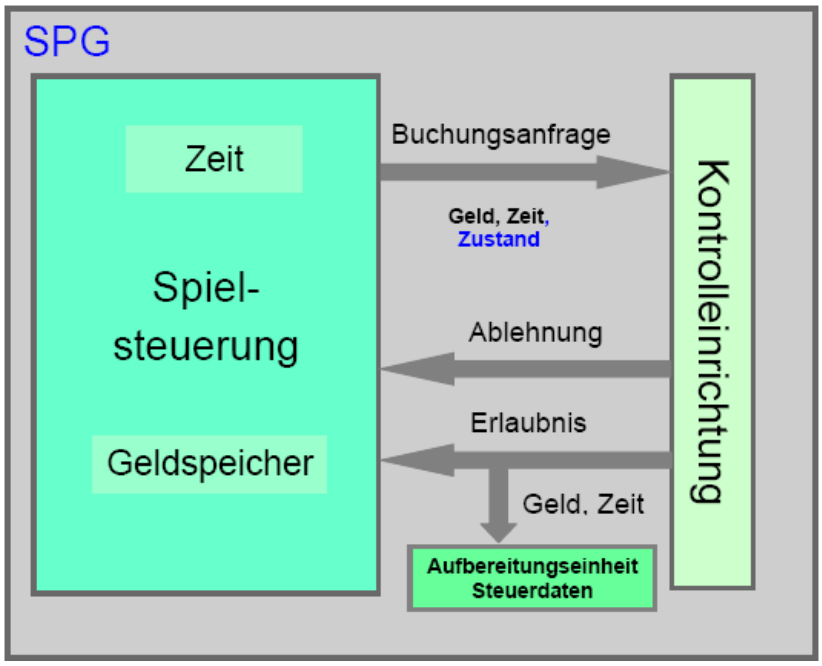



Bild 3: Logischer Aufbau

Die Kontrolleinrichtung wird auf Seite 21 der „Technischen Richtlinie“ [ptb2] folgendermaßen definiert:

*„Alle beabsichtigten Aktionen - Einsatzleistung, Gewinnauszahlung und Zustandsänderung (bzw. –meldung) - werden der Kontrolleinrichtung vor der Ausführung in Form einer Buchungsanfrage zur Prüfung vorgelegt. Sind die Anforderungen erfüllt, wird eine interne Buchung ausgeführt und die Erlaubnis (’Y’ bzw. ’y’) zur Durchführung erteilt. Einsätze und Gewinne werden mit Zeitangabe an die Verarbeitungseinheit zur Aufbereitung der steuerlichen Erhebungen weitergeleitet. Bei erkanntem Regelverstoß erfolgt die Ablehnung der Buchungsanfrage(’N’ bzw. ’n’) gegenüber der Spielsteuerung (siehe Abschnitt 5).“*

D.h., die PTB erwartet von einer durch Dritte implementierte und für die PTB in der Praxis nicht direkt einsehbare Software, dass diese eine bestimmte Verhaltensweise einhält: unter anderem die von der PTB festgelegten Kontroll- und Überwachungsfunktionen.

Dazu gibt es drei Prüfungskonfigurationen der PTB, die jedes nachgebaute Gerät aufweisen muss und die im Rahmen des Zulassungsverfahrens zur Überprüfung u. a. der Kontrolleinrichtung herangezogen werden.

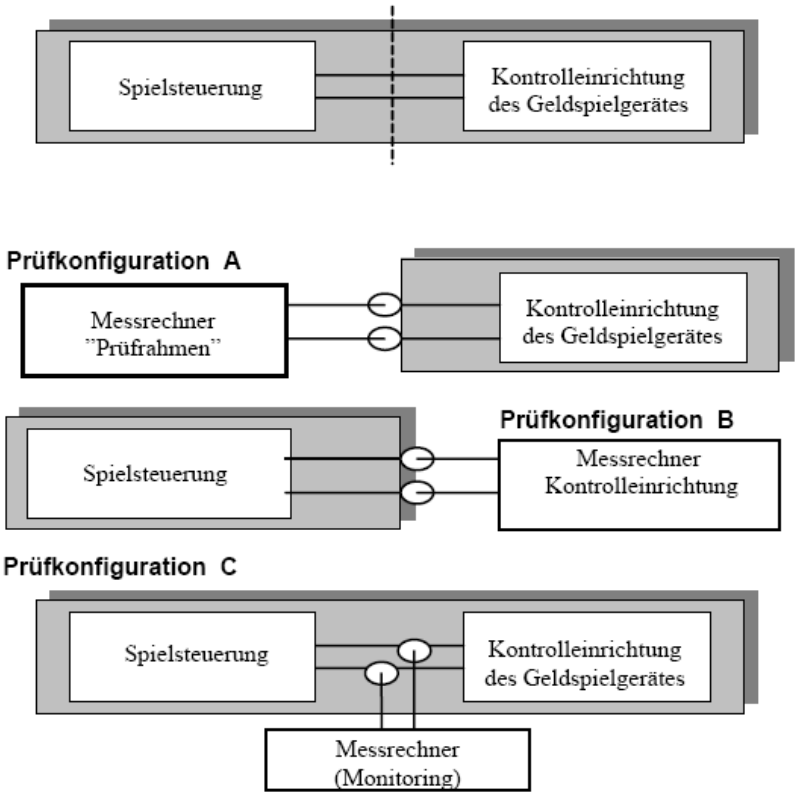



Bild 4: Prüfkonfigurationen der PTB

Der folgenden Tabelle aus [ptb2] kann entnommen werden, dass das Einleiten einer „Messung“ dem Geldspielgerät mittels Steuersequenzen mitgeteilt und dessen „Kooperation“ benötigt wird.

**Tabelle 6: Übertragungs-Steuersequenzen**

| Sender | Steuersequenz | Bedeutung |
|---|---|---|
| SPG | ESC '**P**' *p* LF | Leitet unmittelbar nach P das Senden der Gerätekenndaten *p* ein. LF schließt die Sequenz ab. (Bedeutung und Codierung von *p* siehe Tabelle 8) |
| MR<br>SPG | ESC '**M**' *s* LF<br>ESC '**M**' *s* LF | Aufforderung zur Einstellung der Prüfkonfiguration *s*<br>Bestätigung der Einstellung der Prüfkonfiguration *s*<br>(Bedeutung und Codierung von *s* siehe Tabelle 7) |
| SPG | ESC '**D**' LF | Leitet (in Prüfkonfiguration B und C) das unmittelbar folgende Senden des Geldverfügungsspeicher-Stands ein. |
| SPG | ESC '**E**' LF | Teilt (in Prüfkonfiguration A) die Empfangsbereitschaft der KE mit. Es können nacheinander vom MR Buchungsanfragen empfangen werden solange bis ein Abbruchsignal eintrifft. |
| SPG | ESC '**F**' LF | Meldung, dass ein fehlerhaftes Signal empfangen wurde. |

Tabelle 1: Steuersequenzen der Prüfkonfigurationen

# 5 Die Ist-Situation

## 5.1 Bauartprüfung

§ 13 SpielV gibt explizit vor, welche Anforderungen an ein Geldspielgerät erfüllt sein müssen, damit eine Bauartzulassung durch die PTB erteilt werden darf [spielv1].

Zusätzlich hat die PTB die „Technische Richtlinie – Zur Sicherung der Prüfbarkeit und Durchführung der Bauartprüfung von Geldspielgeräten im Sinne von § 33c Gewerbeordnung“ [ptb2] erlassen.

Bei erfolgreicher Bauartprüfung erteilt die PTB dem Hersteller eine Bauartzulassung.

Damit ist der Hersteller berechtigt, Nachbaugeräte entsprechend dem Bauartmuster herzustellen.

## 5.2 Herstellung

Die Nachbaugeräte werden ohne weitere Überprüfung durch Dritte vom Hersteller ausgeliefert.

## 5.3 Aufstellung

Die Geräte können über Händler oder direkt an die Aufsteller gelangen.

Die Aufsteller können freie Aufsteller oder auch Spielsalonketten der Hersteller selbst sein.

Die Geräte werden teilweise nur noch vermietet oder verleast.

Die Hersteller bieten bzw. verlangen eine Anbindung der Geräte per LAN-Schnittstelle an ein Netzwerk, welches dann auch mit einem zentralen Server des Herstellers verbunden sein kann.

Die Geräte sind für die Spielhallenbetreiber, welche auch die Hersteller sein können, per Schlüssel jederzeit zu öffnen.

## 5.4 Freischaltung

Um ein Gerät überhaupt in Betrieb nehmen zu können, muss im Geräteinneren eine Chipkarte in einen Kartenleser gesteckt werden, und diese muss vom Gerät akzeptiert werden. Dies erfolgt in der Regel durch den Aufsteller.

## 5.5 Zugelassener Betrieb

Ferner befinden sich im Geräteinneren die von der PTB geforderten Prüfschnittstellen, je nach Hersteller bzw. Bauart eine versiegelte „Datenbank“ oder gesteckte EPROM, LAN- und USB-Schnittstellen sowie der allgemein freie Zugang zu Platinen, Steckern, Kabeln und weiteren Baugruppen wie Netzteil, Münzprüfer etc.

Über eine der Schnittstellen erfolgt das Abrufen von Abrechnungsdaten zur Erstellung eines Kontrollstreifens für das Finanzamt. Wird dieser Streifen gefälscht, so sei diese Fälschung lediglich vom Hersteller über dessen „Großrechner“ durch eine nachträgliche statistische Analyse des abgerechneten Spielverhaltens nachweisbar [adp5].

Ebenfalls über eine Schnittstelle können, abhängig von der Bauart der Geräte, Softwareupdates von dem Personenkreis mit Zugang zum Geräteinneren aufgespielt werden.

Für einzelne Baugruppen, insbesondere die Münzspeicher, sind teilweise kryptografische Verfahren für die Datenübertragung mit der Hauptplatine gefordert, die jedoch nicht Gegenstand der vorgegebenen Überprüfung sind.

### 5.6 Prüfung nach erfolgter Aufstellung

Alle zwei Jahre soll ein Aufsteller sein Gerät laut PTB „auf Bauartkonformität nach §7 SpielV“ überprüfen lassen [ptb1], laut Gesetzgeber und § 7 SpielV hingegen „auf Übereinstimmung mit der zugelassenen Bauart“ [spielv2].

Erhält ein Gerät keine Prüfplakette, egal aus welchem Grund, führt dies zu keinerlei weiteren Maßnahmen, Meldungen o.Ä.

Ob ein Gerät zu überprüfen ist, wird von keiner zentralen Instanz aktiv überwacht, sondern dem Aufsteller überlassen, und unterliegt der Kontrolle von örtlichen Behörden der Bundesländer.

Für geleaste oder gemietete Geräte könnten Prüfinstanz und –gebühr vom Hersteller/Vermieter vertraglich festgeschrieben werden.

Mindestens ein Hersteller (adp) hat bereits eine vertragliche Vereinbarung mit dem TÜV Rheinland zur Geräteüberprüfung, sodass hier wirtschaftliche Interessen als Gegenstand einer Prüfung im Raum stehen, die von angestellten, weisungsgebundenen Prüfern umgesetzt werden sollen [adp1].

## 5.7 Prozessdiagramme Ist-Prozess

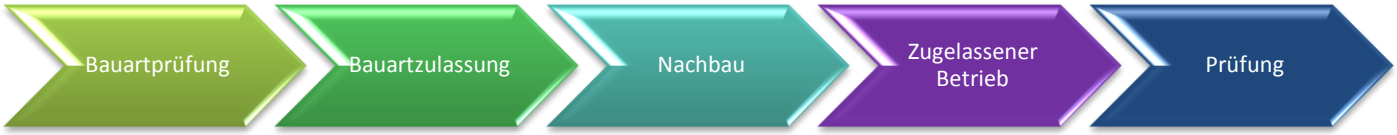



Bild 5: Prozessdiagramm von Zulassung bis Überprüfung

Der allgemeine Prozessablauf von der Bauartprüfung bis hin zur Prüfung zwei Jahre nach erfolgtem Betrieb ist, bezogen auf die einzelnen Prozessblöcke, zeitlich linear ausgelegt. D.h., der Prozess besitzt keine Vorkehrungen, um Sicherheitsprobleme in einem Prozessabschnitt an vorhergehende Prozessabschnitte zurückzumelden.

Es handelt sich im Grunde um einen einfachen „Wasserfall-Prozess“ ohne iterative oder rekursive Zustände zur Erkennung und Behebung von Problemen.

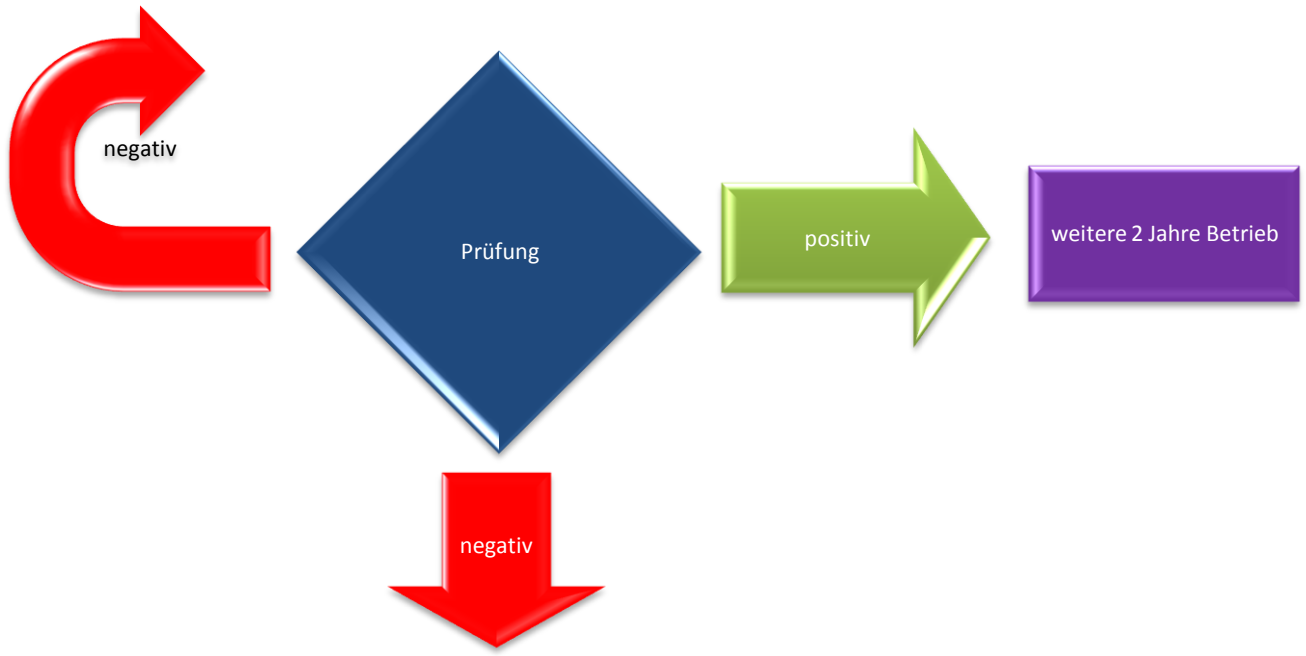



Bild 6: Prozessdiagramm der Prüfung

Innerhalb der Prüfung (als eigener Prüfprozess betrachtet) sieht der Zustand einer negativen Prüfung lediglich eine weitere Prüfung oder einen unerwünschten Zustand (Betrieb ohne Prüfung und damit ohne Zulassung) vor.

Ähnliches gilt letztlich für die Aufstellung, auf die nicht notwendigerweise der Zustand einer Prüfung nach zwei Jahren erfolgen muss, sondern ebenfalls ein unerwünschter Zustand (Betrieb ohne Prüfung und damit ohne Zulassung) möglich ist.

Das folgende Zustandsdiagramm zeigt diesen aus sicherheitstechnischer Sicht offensichtlichen Fehler im Prozess.

## 5.8 Zustandsdiagramm Ist-Prozess

Die Tabelle zeigt die möglichen Zustände, die ein nachgebautes Gerät einnehmen kann:

| Zustand | Legende |
|---|---|
| Herstellung | H |
| Aufstellung | A |
| Freischaltung | F |
| Zugelassener Betrieb | Z |
| Prüfung | P |
| Nicht zugelassener Betrieb | N |
| Außer Betrieb | X |

Tabelle 2: Zustände eines Geldspielgeräts nach PTB-Richtlinien

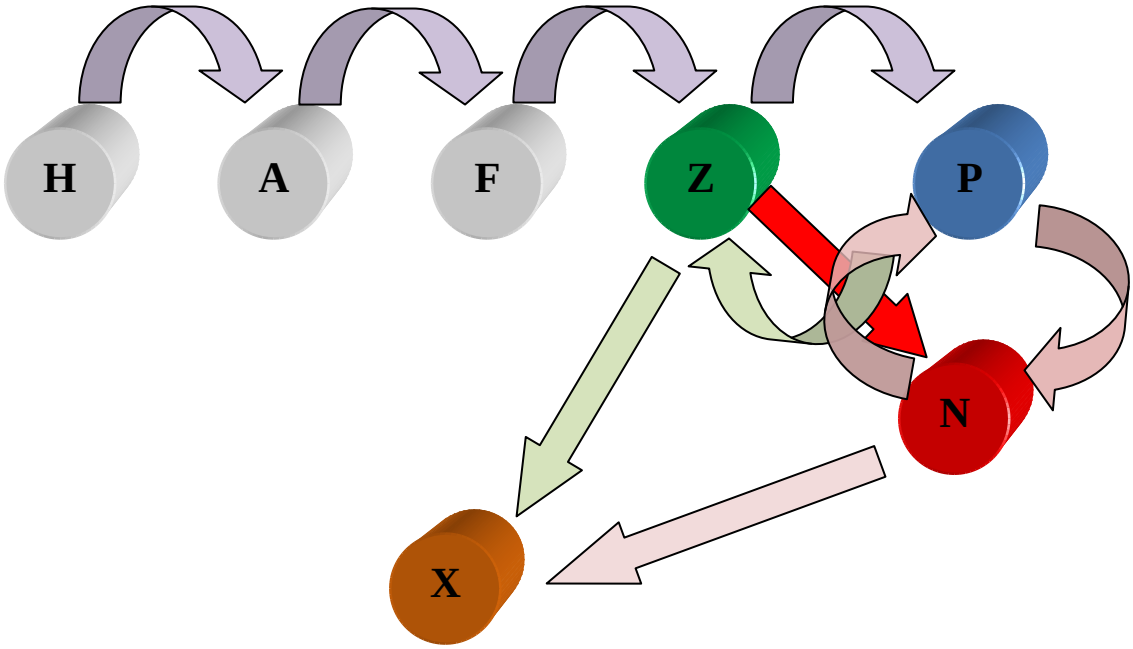



Bild 7: Zustandsdiagramm eines Geldspielgeräts nach PTB-Richtlinien

Das Zustandsdiagramm zeigt deutlich, dass ein Gerät bereits ohne Berücksichtigung irgendwelcher Sicherheitsrisiken direkt nach zwei Jahren in einen nicht zugelassenen Betrieb übergehen und in diesem Zustand undefiniert verbleiben kann, ohne dass dies vom Prozess verhindert wird.

Laut [dbt1] Seite 4, Absatz 1 übernimmt die PTB keine Überwachungsfunktion und überlässt diese den örtlichen Behörden der Bundesländer. Da der Prozess keinerlei Zustand vorsieht, eine solche Kontrolle einzubinden, darf der von der PTB vorgegebene Prozessverlauf als vollkommen eigenständig betrachtet werden, ohne Einflussnahme von oder nach außen.

# 6 Begriffsdefinitionen und Erläuterungen

In diesem Kapitel werden die im Weiteren verwendeten Begriffe erklärt und definiert.

## 6.1 Begriffserklärung „Geldglücksspielgerät“

Das Geldglücksspielgerät (Gerät) besitzt alle wesentlichen Komponenten eines üblichen Computers, teilweise jedoch ohne Festplattenspeicher.


Bild 8: Die wesentlichen Gerätekomponenten

Dem Diagramm kann bereits entnommen werden, dass es zur Manipulation eines Geräts auf jeden Fall einer entsprechenden Anwendungssoftware bedarf, die mehr kann, als nur das Glücksspiel zu simulieren. Erst wird eine im Gerät befindliche Anwendung benötigt, welche letztlich die missbräuchliche Kommunikation mit Hardwareschnittstellen bewerkstelligen kann.

Solange die Anwendungssoftware ausschließlich das macht, was sie soll, könnten Hardware und Betriebssystem zunächst beliebige Sicherheitslücken aufweisen. Allerdings können über Sicherheitslücken im Betriebssystem sowohl die vorhandene Software ersetzt bzw. verändert werden, wie auch zusätzliche Software eingespielt und zur Anwendung gebracht werden.

Besitzt auch das Betriebssystem nur die notwendigsten Komponenten, müsste zusätzlich zur Anwendungssoftware auch das Betriebssystem ersetzt bzw. ergänzt werden, um Sicherheitslücken in der Hardware ausnutzen zu können.

Je weniger Schnittstellen die Hardware physikalisch aufweist, desto weniger kann über die Anwendungssoftware oder das Betriebssystem bewerkstelligt werden.

## 6.2 Begriffserklärung „Beteiligte Parteien“

Das folgende Bild zeigt die am Ist-Prozess beteiligen Parteien und wie der Ist-Prozess das Risiko gewichtet:

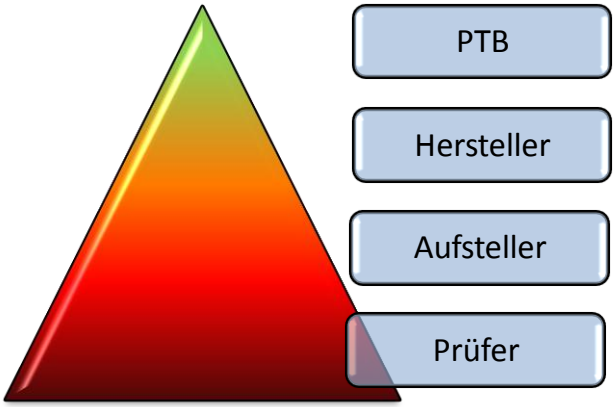



Bild 9: Risikopyramide Ist-Prozess

Der Ist-Prozess sieht lediglich ein zunehmendes Risiko von der Bauartzulassung über die Herstellung und Inbetriebnahme bis hin zum Zeitpunkt der Prüfung vor. Das größte Risiko besteht ab der Aufstellung und nimmt mit zunehmender Betriebszeit und Anzahl nachgebauter Geräte zu. Dies reflektiert auch der Zeitpunkt der Prüfung, wie in 5.8 gezeigt. Bauartzulassung und Nachbau werden zumindest im Ist-Prozess nicht als hohes Risiko betrachtet, sonst gäbe es hierfür aktive Kontrollmechanismen.

## 6.3 Begriffsdefinition „Sicherheit“

Der Sicherheitsgedanke beschränkt sich in dieser Arbeit ausschließlich darauf, einen Zulassungs- und Prüfprozess umzusetzen, der maximale Sicherheit vor vorsätzlichen oder auf Fehlern beruhenden Gerätemanipulationen am Prozess Beteiligter (PTB, Hersteller, Aufsteller, Prüfer) bietet.

Am Prozess indirekt Beteiligte wie PTB-, Hersteller- und Aufstellermitarbeiter fließen eigens in die Sicherheitsbetrachtung ein.

Am Prozess unbeteiligte Dritte wie Händler, Spieler, Diebe oder Betrüger können nur Schaden anrichten, den Beteiligte am Prozess oder deren Mitarbeiter zu verantworten haben und finden deshalb keine weitere Berücksichtigung in der Begriffsdefinition, Risiko- und Schadensbetrachtung.

Als Geschädigte werden weder Beteiligte noch sonstige Personenkreise betrachtet. Es wird ausschließlich der Schaden für die Zielsetzung des Prozesses betrachtet.

### 6.4 Begriffsdefinition „Risikobewertung“

Eine Einzelbetrachtung der Beteiligten (siehe 7.2 ff.) zeigt, dass die Risikoeinschätzung deutlich differenzierter ausfallen muss, wenn ein sicherer Prozess angestrebt werden soll. Denn tatsächlich besitzen sowohl die PTB wie auch die Hersteller gleichermaßen und teils unabhängig voneinander das Potenzial, jederzeit einen neuen Schaden im Sinne von 6.3 zu verursachen, der große Teile des Marktes betrifft, zum Beispiel durch die fehlerhafte Zulassung eines Geräts oder einen nichtzulässigen Nachbau.

Aufsteller hingegen können nur unter Ausnutzung durch PTB oder Hersteller zu verantwortende Risiken einen Schaden anrichten, wie Fälschung von Abrechnungen oder Betrug durch Ausnutzung von Geräteschwachstellen.

Schäden, die ein einzelner unabhängiger Prüfer verursachen könnte, sind gering. Erlaubt aber das Zulassungsverfahren für Prüfer einen direkten Zusammenhang zu einem Aufsteller, Hersteller oder PTB, steigt die Gefahr von Subjektivität entsprechend und somit das Schadenspotenzial.

Die grundsätzliche Bewertung des Risikos beruht deshalb auf folgenden Einzelüberlegungen:

1. **Sehr hoch**: Das maximale Schadensrisiko besteht darin, dass alle Hersteller gezielt Geräte in Umlauf bringen können, die ihnen illegale Manipulationen erlauben, die nicht kontrolliert, geprüft oder nachgewiesen werden (können).
2. **Hoch**: Bei nur drei wesentlichen Herstellern am Markt (siehe 7.3) besteht das Risiko, dass es einem Hersteller ermöglicht wird, gezielt Geräte in Umlauf zu bringen, die ihm illegale Manipulationen erlauben, die nicht kontrolliert, geprüft oder nachgewiesen werden können.
3. **Mittel**: Weniger schadensträchtig ist ein Fehler in der Bauartzulassung oder beim Nachbau, wenn dieser unbeabsichtigt entstanden ist und weder von der PTB noch von Herstellerseite gewünscht ist. Es entsteht ein Schaden durch die Ausnutzung der Fehler und durch die Kosten für ihre Behebung. Diese Art Fehler wurden in der Vergangenheit schnell erkannt und behoben.
4. **Mittel**: Mittelmäßig ist das Schadensrisiko bei den Aufstellern, da diese entweder einen kleinen Wirkungskreis besitzen oder als Herstellerketten bereits unter Punkt 2 berücksichtigt werden.
5. **Mittel**: Mittelmäßig ist das Schadensrisiko bei Manipulationen durch Herstellermitarbeiter, insbesondere wenn sie eine Vertrauensposition genießen oder den Qualitätssicherungsprozess des Herstellers umgehen können.
6. **Gering**: Gering ist das Schadensrisiko bei Manipulationen durch Aufstellermitarbeiter oder der Ausnutzung von Insider-Informationen zu Manipulationen, da diese entweder in der Vergangenheit schnell erkannt und abgestellt wurden oder lediglich einen Aufsteller betreffen.
7. **Mittel**: Das Schadensrisiko durch Prüfer ist gegeben. Zwar sollte ein Prüfer nicht mehr als 10 bis 15 Geräte am Tag prüfen können, bei mangelnder Unabhängigkeit könnten jedoch deutlich mehr „pro forma“-Prüfungen durchgeführt werden.
8. **Hoch**: Wird jedoch ein Hersteller alle Geräte unter seiner Kontrolle von einer vertraglich gebundenen zugelassenen Stelle prüfen lassen, bedeutet das ein flächendeckendes Risiko. Dabei darf unterstellt werden, dass kein Hersteller eine zugelassene Stelle beanspruchen wird, die bereits mit einem anderen Hersteller vertragliche Bindungen hat.

Dass die Risiken und deren Einstufung durchaus realistisch sind, wird anhand konkreter Beispiele in den Einzelbetrachtungen (siehe 7) belegt.

### 6.5 Begriffsdefinition „mögliche Risiken“

Um das Sicherheitsrisiko konkreten Handlungen bzw. Motiven zuweisen zu können, werden folgende Begriffe aus 6.4 abgeleitet:

- Umgehung der Sicherheitsmaßnahmen
- Bevorzugung eines Herstellers
- unbeabsichtigte Fehler
- persönliche Bereicherung Einzelner
- Manipulationen durch Aufsteller
- Manipulationen durch Sachverständige
- Manipulationen durch zugelassene Stellen

Das größte Risiko, das komplette **Umgehen aller Sicherheitsmaßnahmen**, besteht dann, wenn bei der PTB eine allgemeine Sicherheitslücke bei Zulassungs- und Prüfverfahren entsteht welche die Hersteller für ihre eigenen Ziele ausnutzen können, oder wenn alle Hersteller, unabhängig von der PTB, beispielsweise ihre Geräte absichtlich so konstruieren könnten, dass diese jederzeit mit Herstellerwissen manipulierbar wären.

Die **Bevorzugung eines Herstellers** folgt der Überlegung, dass nicht alle Hersteller in diese „bevorzugte“ Situation kommen können. Es wird dabei unterstellt, dass sich kein Hersteller aus Wettbewerbsgründen eine Möglichkeit zur Vorteilsverschaffung entgehen lassen würde, wenn ein Mitbewerber diese bereits besitzt. Damit könnte die beschriebene Situation nur durch einzelne Mitarbeiter die PTB im Zusammenspiel mit einem Hersteller herbeigeführt werden.

**Unbeabsichtigte Fehler** sind von allen Beteiligten ungewollte Fehler in der Zulassung oder Herstellung.

Die **persönliche Bereicherung** ist ein Sicherheitsrisiko, welches durch die Mitarbeiter von am Prozess Beteiligten entsteht, und kann von Fälschung und Betrug bis über das direkte bzw. indirekte Ausnutzen von vertraulichen Informationen oder einer vertraulichen Position reichen.

**Manipulationen durch Aufsteller** sind Manipulationen, Fälschungs- oder Betrugsmethoden, die als allgemeine Geschäftspraxis eines Aufstellers praktiziert werden.

**Manipulationen durch Sachverständige** beziehen sich auf das missbräuchliche Vergeben oder Enthalten von Prüfplaketten.

**Manipulationen durch zugelassene Stellen** beziehen sich auf das missbräuchliche Vergeben oder Enthalten von Prüfplaketten der zugelassenen Stellen aus wirtschaftlichen Erwägungen mittels ihrer weisungsgebundenen und wirtschaftlich abhängigen Mitarbeiter.

Diese Form der Betrachtungsweise erlaubt das Reduzieren vieler denkbarer Einzelrisiken auf „verursachende“ Risiken. Beispielsweise besteht einerseits das Risiko, dass ein Gerät in einen nicht zugelassenen Betriebszustand verfallen kann, andererseits wird dieses Risiko automatisch mit dem Risiko der Umgehung von Sicherheitsmaßnahmen behoben.

Im Rahmen von Einzelbetrachtungen (siehe Kapitel 7) werden die Risiken detailierter betrachtet.

# 7 Einzelbetrachtungen der Sicherheitsrisiken

## 7.1 Einzelbetrachtung des Risikofaktors „Gerät“

Ausgehend von der Situation des Prüfers, der nach §7 SpielV die Überprüfung der Übereinstimmung mit der zugelassenen Bauart vorzunehmen hat, wozu nach Vorgabe der PTB das Ermitteln der CRC32-Checksumme über eine Schnittstelle im Gerät oder ausgelesene EPROM bzw. CF-Karten gehört, lassen sich die einzelnen Problembereiche des Prüfverfahrens aufzeigen, zunächst unabhängig davon, ob diese bereits adäquat abgesichert sind oder nicht.

### 7.1.1 Die Prüfung des Binärcodes

Abschnitt 3 von [ptb1] besagt:

*Diese äußere Prüfung wird bei der Geräteinspektion durch einen Checksummenvergleich vertieft. Dazu ist der Binärcode der Software auszulesen, extern eine Checksumme nach einem im Zulassungsschein benannten Verfahren zu berechnen und mit der veröffentlichten Checksumme zu vergleichen. Falls die zur Bauart gehörende Software und entsprechende Speicherdaten auf mehrere Hardwarebausteine verteilt sind, erfolgt der Checksummenvergleich für die jeweiligen Hardwarebausteine getrennt. Bei Verwendung von Betriebssystemkernen sind bestimmte Daten veränderlich. Betreffende Bereiche sind aus dem Vergleich auszunehmen. Ebenso sind bestimmte Softwareteile, die nicht die Eigenschaften der Bauart beeinflussen (z. B. bestimmte Graphiksoftware) aus dem Vergleich ausgenommen.*

Aktuell wird CRC32 [ptb4] für den Checksummenvergleich in den Zulassungsscheinen angegeben.

CRC32 ist dazu geeignet festzustellen, ob bei einer erfolgten Datenübertragung fehlerhafte Bits entstanden sind und somit die übertragene Datei als korrupt betrachtet werden muss. Für eine weitergehende Aussage bezüglich der Übereinstimmung zweier Dateiinhalte ist CRC32 definitiv nicht geeignet, da ausgehend von einem bekannten CRC32-Wert sehr einfach weitere Datenströme mit demselben CRC32-Wert erzeugt werden können (siehe 9.6).

Das bestehende Prüfverfahren könnte mit CRC32 höchstens eine Aussage darüber zulassen, ob der ausgelesene Datenstrom fehlerhaft übertragen wurde.

Kapitel 1.2 Entwicklungsstandards der „Technischen Richtlinie“ [ptb2] lässt eine Offenlegung des kommentierten Sourcecodes für die Bauartzulassung zumindest vermuten:

*Die Bauart entspricht in ihrer Konstruktion dem Stand der Technik. Die eingesetzten Bauteile und verwendeten Verfahren bieten die Gewähr, dass die Geldspielgeräte bestimmungsgemäß funktionieren.*
*Die Software wurde unter Beachtung der anerkannten Regeln des Softwareengineering entwickelt. Insbesondere ist sie angemessen dokumentiert und kommentiert.*

Es ist nicht die Rede davon, dass das Quellprogramm kompiliert und das Ergebnis mit dem Objektcode im Baumuster verglichen wird.

Das Auslesen des Binärcodes erfolgt über die zwei Varianten „Binärcode über eine Geräteschnittstelle auslesen“ bzw. „EPROM/CF-Karte ausbauen und Binärcode auslesen“, je nach Bauart des Geräts.

Das Auslesen über eine Geräteschnittstelle überträgt eine Binärdatei auf den PC des Prüfers im laufenden Betrieb des Geräts. Es ist damit weder eine Aussage darüber möglich, ob die ausgelesene

Datei tatsächlich dem bei der PTB hinterlegten Binärcode entspricht, noch ob die ausgelesene Datei auch tatsächlich im Gerät ausgeführt wird. Dazu ist der Einsatz von einer jeweiligen Herstellersoftware zwingend erforderlich. Im Falle des Herstellers NSM wird diese Software sogar individuell für jeden Sachverständigen kompiliert.

Bei Geräten mit EPROM oder CF-Karte könnte es sich lediglich um Speicherbausteine handeln, deren Binärcode vom Gerät gar nicht zwingend benutzt wird, wenn die verbaute Hardware einen RAM-Speicher aufweist, der auch weitere Software aufnehmen und ausführen kann.

In beiden Fällen könnte mit Schnittstellen für externe Dateneinspielung im laufenden Betrieb der ausgeführte Binärcode ein anderer sein, als der durch den Prüfer vom Gerät ausgelesenen und geprüften. D.h., auch ein sicheres kryptografisches Verfahren anstelle von CRC32 oder gar ein direkter Vergleich der bei der PTB hinterlegten und mit den vom Prüfer ausgelesenen Binärdaten bieten keine Sicherheit.

**Sicherheitseinstufung**

Die in [ptb1] erwähnte Vertiefung der Prüfung ist aus technischer bzw. sicherheitstechnischer Sicht nicht erkennbar. Der Checksummenvergleich des Binärcodes darf für Geräte, die CRC32 in ihrer Bauartzulassung verlangen, als ungeeignet und höchst unsicher eingestuft werden.

Ebenso bietet das Auslesen des Binärcodes keinerlei Grundlage für eine Sicherheitsprüfung, da das offensichtliche Risiko darin besteht, dass im laufenden Betrieb veränderte Software nachträglich eingespielt werden kann. Oder es könnten EPROMs mit veränderter Software eingesetzt werden, die vor der Prüfung gegen EPROMs mit korrektem Inhalt ausgetauscht wurden.

Die Bauartzulassung sieht nicht vor, dass der Objektcode im Baumuster und späteren Gerät mit einem aus dem Sourcecode kompilierten Objektcode verglichen wird.

Auch wenn sowohl Sourcecode wie auch Objektcode bei der Bauartzulassung durch die PTB eingehend geprüft würden, kann das Prüfverfahren nach der Aufstellung keinerlei Sicherheit darüber geben, ob ein Gerät auch wirklich mit dieser Software betrieben wird.

Erschwerend kommt noch hinzu, dass bereits ein einfacher Reset/Reboot-Mechanismus oder eine Port-Überwachung ausreichen würde, ein Gerät in einen definierten (sprich: zugelassenen) Zustand zu versetzen.

Die vorgegebene Prüfung des Binärcodes ist kein wirksamer Sicherheitsmechanismus.

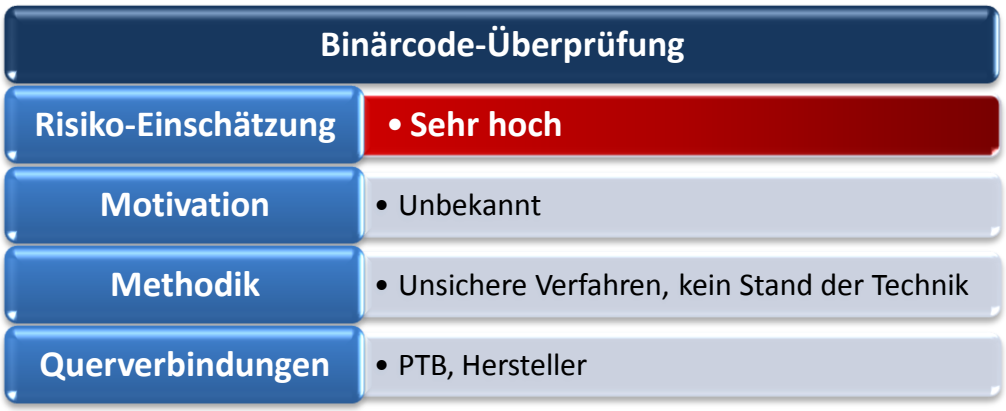



Bild 10: Risikoeinschätzung der Binärcode-Überprüfung

### 7.1.2 Die Gerätehardware

Die Hardware wird von den Geräteherstellern selbst festgelegt. Sie verfügt heutzutage über LAN-Schnittstellen, serielle Ports, herausnehmbare EPROMs, Kartenlesegeräte etc. In der „Technischen Richtlinie – Zur Sicherung der Prüfbarkeit und Durchführung der Bauartprüfung von Geldspielgeräten im Sinne von § 33c Gewerbeordnung“ [ptb2] sind keine weiteren Vorgaben oder Auflagen zur Absicherung der Hardware vorgeschrieben. Somit könnte diese - vom Prüfer unerkannt bzw. für den Prüfer nicht von Belang – Eigenschaften aufweisen, die weder per Sicherheits-Hardware noch per Software überprüfbar sind.

§ 13 (1) 10 SpielV verlangt explizit von der PTB als Zulassungskriterium einer Bauart [spielv1]:

*Das Spielgerät muss so gebaut sein, dass die Übereinstimmung der Nachbaugeräte mit der zugelassenen Bauart überprüft werden kann.*

Das legt zumindest aus technischer Sicht nahe, dass die „Technische Richtlinie“ eine ergänzende Informationen darstellt und deshalb von der PTB keine Verplombung, Verdongelung oder ähnliche Maßnahme in [ptb2] explizit genannt werden, um die verbaute Hardware gegenüber dem Bauartmuster zu verifizieren. Es wäre zu erwarten, dass fehlende herstellerseitige Maßnahmen oder Geräteeigenschaften, die eine sinnvolle Überprüfung verhindern, zu einer Nichterteilung der Bauartzulassung durch die PTB führen. Dies ist aus technischer Sicht durch die in 7.1.1 aufgezeigten Überprüfungsmethoden jedoch nicht gegeben.

Vielmehr sind die Geräte so konstruiert und zugelassen worden, dass sogar eine aktive Entziehung einer Überprüfung als Schadensszenario in Frage kommt. Dies führt dazu, dass herkömmliche Sicherheitsmechanismen, die minimale Hardwareänderungen erkennen und darauf reagieren (wie etwa in Microsoft-Produkten vorkommend), als nachträglicher Manipulationsschutz nicht mehr implementierbar sind, da sie aufgrund der in 7.1.1 dargestellten Unsicherheitsfaktoren jederzeit ausgehebelt werden könnten.

Zusätzlich werden z. B. in Geräten von adp sogenannte „Datenbanken“ verbaut [adp2], welche im Wesentlichen aus gepufferten Speicherbausteinen bestehen, deren Stromversorgung bei Öffnung des Metallgehäuses ausfällt. Die Sicherheitsmechanismen umfassen Lichtsensoren, Anbohrschutz etc. D.h., die Hersteller verbauen Sicherheitstechnik in ihre Geräte, die nur die Hersteller kontrollieren oder prüfen können und womit auch eine forensische Analyse effektiv behindert würde. Tatsächlich gibt es jedoch Anbieter, die das Öffnen der „Datenbanken“ anbieten [dom1].

Die verbauten Kommunikationsschnittstellen sind explizit für die Kommunikation in beide Richtungen ausgelegt. Die seriellen Prüfschnittstellen reagieren auf entsprechende Befehle, um in die verschiedenen von [ptb2] S. 36 ff. beschriebenen Zustände zu gelangen. Bei adp-Geräten können Updates über die serielle Schnittstelle eingespielt werden [adp2]. Die LAN-Schnittstellen werden u. a. dazu benutzt, die Geräte über Fernwartung zu steuern [adp3], was eine entsprechende Softwareschnittstelle im Betriebssystem voraussetzt.

Die Antwort der Deutschen Bundesregierung auf die kleine Anfrage " Drucksache 16/5687“ [dbt1] bezieht sich auf einen Vorfall, bei dem mehrere tausend Geräte der adp-Spielhallenkette nachträglich mit Zusatzplatinen ausgestattet wurden. Diese wurden zwischen Kartenleser für die Zulassungskarte und Hauptplatine eingeschleift und ermöglichten eine Veränderung des Spielverhaltens (= Kommunikation mit der Software) [uadv1]. Zwar handelte es sich dabei um Geräte, die noch nicht von der aktuellen SpielV betroffen waren, die physikalische Schnittstelle ist jedoch bei neuen Geräten immer noch vorhanden.

**Sicherheitseinstufung**

Die Geldspielgeräte sind auf ihre Übereinstimmung mit der zugelassenen Bauart nicht überprüfbar.

Es sind keinerlei erkennbare Verifikationsmechanismen implementiert, weder in der Software noch in der Hardware. Wären diese tatsächlich vorhanden, könnten sie durch einfache Manipulationen an Hard- oder Software wirkungslos gemacht werden.

Die Bauartzulassung erlaubt herstellerspezifische Sicherheitskomponenten, die eine Überprüfung auf möglichen Missbrauch verhindern und eine forensische Untersuchung erschweren sollen.

Die Kommunikationsschnittstellen sind im Prinzip jedem physikalisch zugänglich, der einen Geräteschlüssel besitzt bzw. Netzwerkzugang zum Gerät erlangen kann.

Die gesamte Gerätehardware besitzt ebenfalls keinen wirksamen Sicherheitsmechanismus.

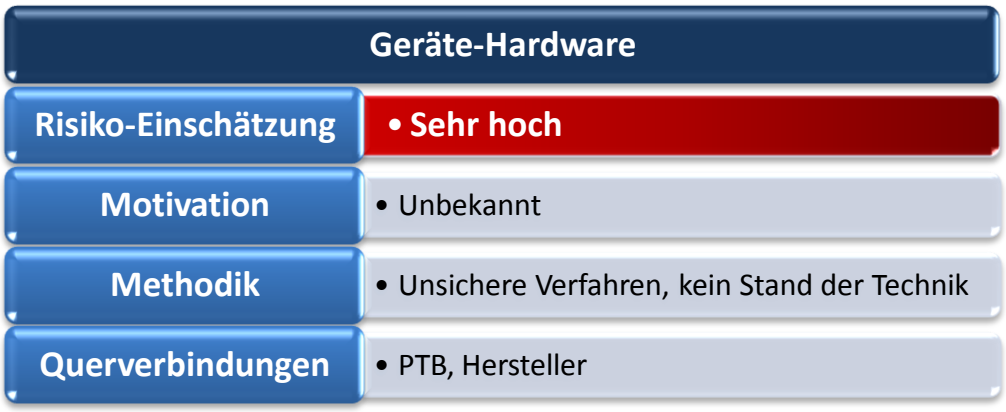



Bild 11: Risikoeinschätzung der Gerätehardware

## 7.2 Einzelbetrachtung des Risikofaktors „PTB“

Im Rahmen der Umsetzung von § 7 SpielV übernimmt die PTB die Aufgabe, einen geeigneten Prozess zur Umsetzung des Zulassungs- und Prüfverfahrens zu entwerfen und zu implementieren. Aus der SpielV [spielv1] ist diese Aufgabenstellung nicht zu entnehmen. Vielmehr wird dort unter IV. SpielV die Zulassung von Spielgeräten zur Aufgabe der PTB deklariert und unter § 7 SpielV die Überprüfung eines Geräts auf Übereinstimmung mit der zugelassenen Bauart u. a. Sachverständigen übertragen. D.h., die PTB organisiert die Überprüfung ihrer Zulassungstätigkeit.

Die PTB stellt als Beteiligte einen Risikofaktor dar, der in einem sicheren Prozess berücksichtigt werden muss:

- Als direkt am Prozess Beteiligte nimmt die PTB auch Einfluss auf das Prüfungsverfahren für Sachverständige und zugelassene Stellen. In [sv4], Seite 25, erklärt sie eine selbst durchgeführte Studie eines PTB-Mitarbeiters als Referenzgutachten für dessen Sachverständigenanwärterschaft, den sie anschließend auch noch geprüft hat.
- Der Ist-Prozess lässt nicht erkennen, dass der „Stand der Technik“ im Bereich IT und IT-Sicherheit umgesetzt wurde, obwohl die Geräte de facto Computer sind.

- Der Ist-Prozess verlangt nach einer hohen Anzahl Prüfer für geschätzte 40.000 zu prüfende Geräte alleine im Jahr 2008, was zu einer erheblichen Steigerung des Risikos in mehrfacher Hinsicht beiträgt.
- Die Prüfung des Binärcodes besitzt keinerlei relevante Aussagekraft.
- Die Messschnittstelle (siehe 4) liefert keine aussagekräftigen Messwerte.
- Die vertraglichen Vereinbarungen mit den Herstellern sind nicht bekannt.
- Der Zulassungs- und Prüfprozess ist abhängig von den Herstellern, deren Geräte Gegenstand der Prüfung sind.
- Bei den Überprüfungen stößt man auf Geräte, die sich trotz korrekten CRC32-Codes anders verhalten als in § 13 SpielV gesetzlich vorgeschrieben.

Die „Technische Richtlinie“ in Version 4.0 [ptb2] zeigt deutlich die Unterschiede zur Vorgängerversion 3.3 auf. Daraus ist nicht zu erkennen, dass das Konzept „Sicherheit“ für den gesamten Zulassungs- und Prüfprozess zwischenzeitlich eine angemessene Bedeutung hätte und das, obwohl in einem PTB-eigenen Gutachten [uadv1] die Risiken aus vergangenen Schadensfällen deutlich erkannt und genannt worden sind.

Ein auffälliges Beispiel hierfür ist die sogenannte Messschnittstelle (siehe 4), mit der lediglich die PTB die Prüfkonfigurationen A, B und C überprüfen darf (siehe [ptb2], Seite 23). Auf den Seiten 30 bis 35 wird in allen Details definiert und ausgeführt, was im Wesentlichen eine einfache serielle Schnittstelle darstellt. Höchst auffällig ist beim Messverfahren jedoch, dass ein Benutzen der Messschnittstelle von der Gerätesoftware erkannt werden muss (siehe [ptb2], Seite 36), womit nicht auszuschließen ist, dass die ausgegebenen Messergebnisse durch Manipulationen der Software verfälscht werden könnten. Dass mit einer solchen Messkonfiguration aussagekräftige Messungen vorgenommen werden können, ist ausgeschlossen.

Deshalb muss die PTB als sehr hohes Risiko eingestuft werden, begründet anhand ihres bestehenden Zulassungs- und Prüfverfahrens, welches als uneffektiv und inhärent unsicher betrachtet werden muss.

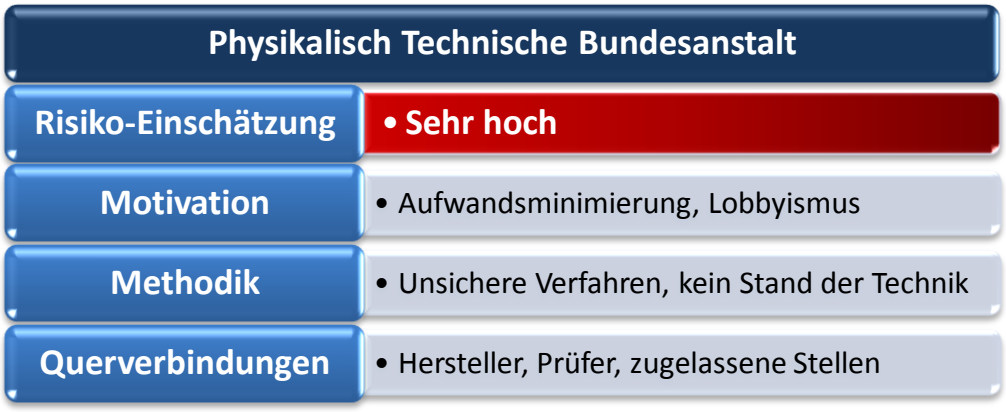



Bild 12: Risikoeinschätzung der PTB

### 7.3 Einzelbetrachtung des Risikofaktors „Hersteller“

Die Hersteller haben einen Verwaltungsvertrag mit der PTB ([dbt1], Seite 3, letzter Satz). Die Hersteller betreiben eigene Spielhallenketten und decken somit die vollständige Wertschöpfungskette ab. Damit stehen sie im direkten Wettbewerb zu den freien Aufstellern, die sie mit Geräten beliefern. Die Geräte werden teilweise nur noch an Aufsteller vermietet oder verleast, wobei die Hersteller eine Anbindung des Geräts per LAN-Schnittstelle an ein Netzwerk bieten bzw. verlangen, welches dann auch mit einem zentralen Server des Herstellers verbunden sein kann. Damit stellt sich die Frage, ob

obige Konstellation bewertbare Risiken birgt, die in einem sicheren Prozess berücksichtigt werden müssen.

- Unter [www1] findet sich ein konkretes Beispiel für einen von einem Gerätehersteller betriebenen Spielsalon im selben Gebäude wie der eines Aufstellers, der die Geräte des Herstellers nicht einsetzt, mit plastischer Schilderung des praktizierten Geschäftsgebarens. Die Verhaltensweise, Filialen möglichst in der Nähe von Konkurrenten zu betreiben, ist eine nicht nur im Geldspielgewerbe verbreitete Praxis.
- Die Version 4 der Technischen Richtlinie enthält unter anderem eine Änderung bezüglich der Spielpausen ([ptb2] 2.4 Spielpause), die nach einer Stunde spielen 5 Minuten betragen sollten. Hersteller wie adp haben den Begriff „Spiel“ als das Aufbrauchen von 20 Cent aus dem Geldspeicher ausgelegt und jedem Spieler vorab so viele Zusatzpunkte in den Punktespeicher gegeben, dass mit diesen Zusatzpunkten das Gerät in den 5 Minuten Zwangspause laufen konnte [adp5]. Das Verbrauchen von Punkten wurde nicht als Spiel gewertet. Die Anpassung an die neue Version 4 klärt diesen Umstand eindeutig, führt aber zu neuen Softwareversionen und damit zu weiteren Risiken.
- Die Vernetzung der Aufsteller mit geleasten bzw. vermieteten Geräten mit Anbindung an zentrale Herstellerserver muss ebenfalls als potenzielles Sicherheitsrisiko beleuchtet werden, da diese Form der Infrastruktur nicht nur generell Risiken birgt, sondern ebenfalls als ideale Plattform für Missbrauch dienen kann ([isa1] zu Pkt. 5).
- Wie in 7.1.2 beschrieben, zeigte ein Hersteller bereits in der Vergangenheit die Bereitschaft, nachträgliche Manipulationen an Geräten vorzunehmen [uadv1].

Diese Beispiele unterstreichen nicht nur die unterschiedlichen Interessen der Hersteller gegenüber den anderen Beteiligten, sondern auch deren Unvereinbarkeit im Rahmen eines sicheren Ablaufs. D.h., der Risikofaktor „Hersteller“ hat sich bereits im Rahmen des Ist-Prozesses bestätigt.

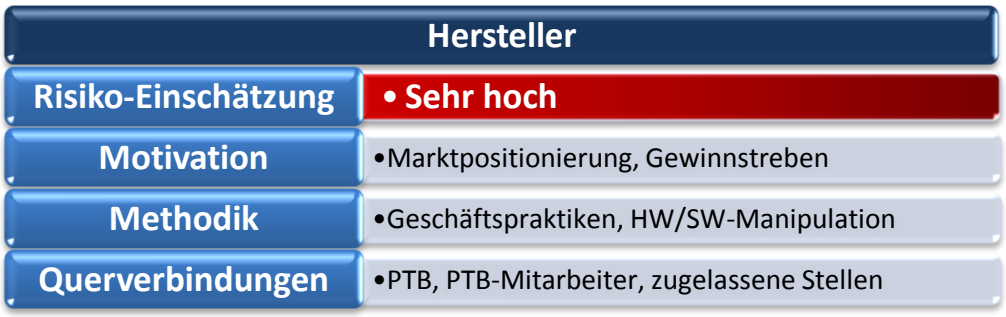



Bild 13: Risikoeinschätzung der Hersteller

## 7.4 Einzelbetrachtung des Risikofaktors „Aufsteller“

Aufsteller besitzen Zugang zum Geräteinneren und führen auch sicherheitskritische Aufgaben wie Abrechnung, Buchhaltung etc. durch. Freie Aufsteller sind frei in ihren Entscheidungen, während die Leiter von Herstellerfilialen zusätzlich einer Kontrolle durch den Hersteller unterliegen. Aufsteller beschäftigen Techniker, Personal in der Administration und direkt oder indirekt Prüfer.

Unter anderem fallen folgende Aufgaben an, die Risiken beinhalten:

- Öffnung des Geräts im Allgemeinen
- Kassieren, Abrechnung und Buchhaltung
- Wartung und Reparatur durch Techniker

- Updates einspielen
- Prüfung beantragen
- Prüfung durch Prüfer

Ein Aufsteller kann direkt oder zusammen mit weiteren Mitarbeitern versuchen, Einfluss auf die Abrechnung, Buchführung und das Kassieren zu nehmen.

Aufsteller können versuchen, selbst oder über Dritte, denen sie Zugang zum Geräteinneren verschaffen, sich Manipulationsmöglichkeiten zu eröffnen.

Eine Manipulation der Hard- oder Software ist prinzipiell denkbar. Die Hürden sind aber deutlich höher anzusetzen als bei den Möglichkeiten, die sich den Herstellern bieten.

Insgesamt beschränkt sich der mögliche Gesamtschaden auf die Geräte des Aufstellers, bis zur Entdeckung der Manipulation.

Größere Schäden, die über Herstellerketten zustande kommen könnten, werden als Teil des Risikofaktors „Hersteller“ eingestuft (7.2).


Bild 14: Risikoeinschätzung der Aufsteller

## 7.5 Einzelbetrachtung des Risikofaktors „Prüfer“

Öffentlich bestellte und vereidigte Sachverständige unterliegen strenger Auflagen, wie § 8 der Sachverständigenordnung [svo1] zu entnehmen ist:

*§ 8 Unabhängige, weisungsfreie, gewissenhafte und unparteiische Aufgabenerfüllung.*

*(9) Der Sachverständige darf sich bei der Erbringung seiner Leistungen keiner Einflussnahme aussetzen, die seine Vertrauenswürdigkeit und die Glaubhaftigkeit seiner Aussagen gefährdet (Unabhängigkeit).*

*(10) Der Sachverständige darf keine Verpflichtungen eingehen, die geeignet sind, seine tatsächlichen Feststellungen und Beurteilungen zu verfälschen (Weisungsfreiheit).*

*(11) Der Sachverständige hat seine Aufträge unter Berücksichtigung des aktuellen Standes von Wissenschaft, Technik und Erfahrung mit der Sorgfalt eines ordentlichen Sachverständigen zu erledigen. Die tatsächlichen Grundlagen seiner fachlichen Beurteilungen sind sorgfältig zu ermitteln und die Ergebnisse nachvollziehbar zu begründen. Er hat in der Regel die von den Industrie- und Handelskammern herausgegebenen Mindestanforderungen an Gutachten und sonstigen von den Industrie- und Handelskammern herausgegebenen Richtlinien zu beachten (Gewissenhaftigkeit).*

Öffentlich bestellte und vereidigte Sachverständige haften ohne Einschränkung für ihre Arbeit. Normalerweise werden Antragsteller ausschließlich von anderen Sachverständigen einer Prüfung unterzogen. Bei der öffentlichen Bestellung für das Sachgebiet 530 (Geldspielgeräte) wird hiervon abgewichen und ein Teil der Prüfung von der PTB vorgenommen und nicht von einer Prüfungskommission aus Sachverständigen. Der Autor kann aus eigener Erfahrung die Feststellung treffen, dass Inhalt und Tiefe der praktischen Prüfung trivialer Natur sind und aus dem Wiedergeben wesentlicher Inhalte einiger Gesetzestexte und inhaltlichen Vorgaben der PTB besteht. Breite und Tiefe der mündlichen Prüfung ist keinesfalls mit den Anforderungen an ein Sachgebiet wie 2100 zu vergleichen.

Neben den öffentlich bestellten und vereidigten Sachverständigen können namentlich benannte Mitarbeiter einer von der PTB zugelassenen Stelle als Prüfinspektoren bestellt werden. Dies sind in der Regel Angestellte eines Unternehmens (z. B. TÜV Rheinland), nicht öffentlich bestellt und vereidigt, nicht unbegrenzt haftbar und letztlich vom Arbeitgeber finanziell abhängig und durch diesen weisungsgebunden. Dass damit ein grundsätzliches Risiko hinsichtlich der Neutralität besteht, spiegelt sich in § 8 des Vertrags zwischen der PTB und einer zugelassenen Stelle wider [ptb5].

Der Ist-Prozess stellt die Anforderungen des Sachgebiets 530 an die Prüfer. Einen sicheren Soll-Prozess zu entwickeln, zu verbessern und zu überprüfen, verlangt jedoch eindeutig die zusätzlichen Qualifikationen des Sachgebiets 2100. Da Sachverständige dieses Sachgebiets bezüglich Geldspielgeräte zudem branchenfremd sind, fließt dies zur Verdeutlichung der Unterschiede in die Risikobewertung mit ein. Denn ein sicherer Soll-Prozess sollte grundsätzlich von den sichersten Prüfern geprüft werden, sofern sich unterschiedliche Risikoabstufungen ausmachen lassen.

- Bei Sachverständigen, die für das Sachgebiet 530 bestellt sind, ergäbe sich außer persönlicher Bereicherung in einigen Fällen auch das Motiv „Geschäftspraktiken“. [sv1], [sv2] und [sv3], [sv4] zeigen Beispiele für öffentliche Bestellungen über die PTB, wo die bestellten Sachverständigen in direktem Kontakt zur Branche stehen und somit Konflikte mit §8 der Sachverständigenordnung niemals auszuschließen sind. Würden beispielsweise im familiennahen Umfeld keine Prüfungen vorgenommen werden ([sv1] und [sv2]), so stellen Prüfungen im Umfeld der Mitbewerber des Familienunternehmens ebenso ein Risiko dar – wobei sich hier die Frage stellt, wen ein Sachverständiger mit wirtschaftlichen Interessen in der Branche denn überhaupt prüfen könnte?
- Bei Mitarbeitern einer von der PTB zugelassenen Stelle ergeben sich zusätzlich die Motive Weisungsgebundenheit und wirtschaftliche Abhängigkeit (siehe [ptb5], § 8).

Bei Sachverständigen, die für das Sachgebiet 2100 bestellt sind, ergeben sich außer für persönliche Bereicherung keine offensichtlichen Motive.

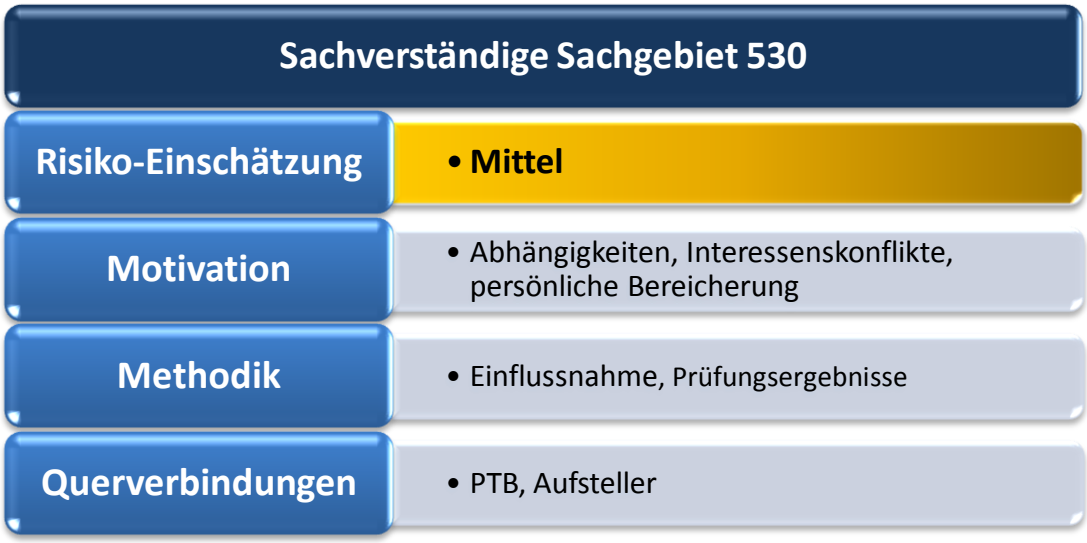



Bild 15: Risikoeinschätzung der Sachverständigen für Geldspielgeräte

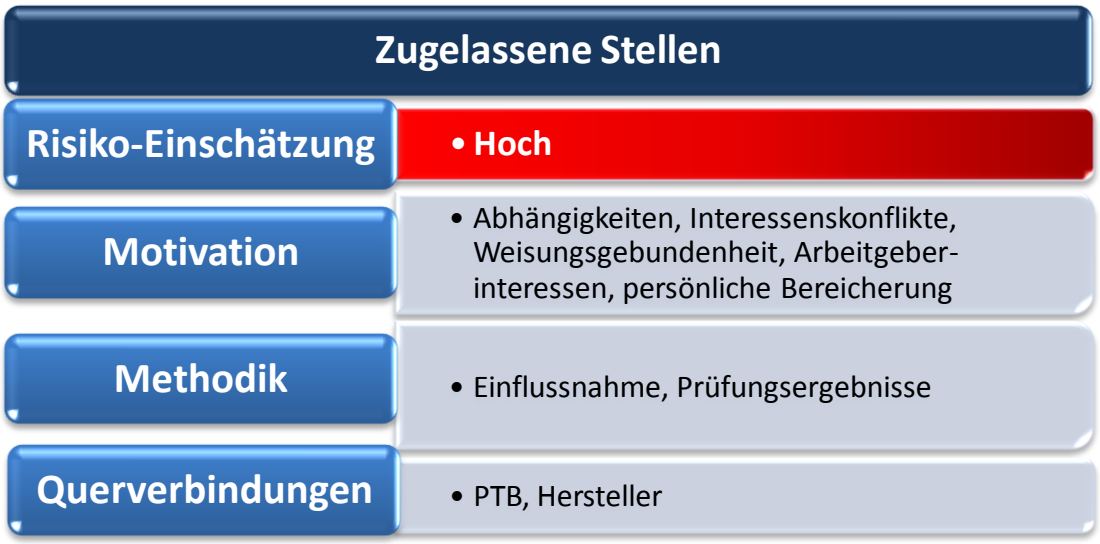



Bild 16: Risikoeinschätzung der von der PTB zugelassenen Stellen

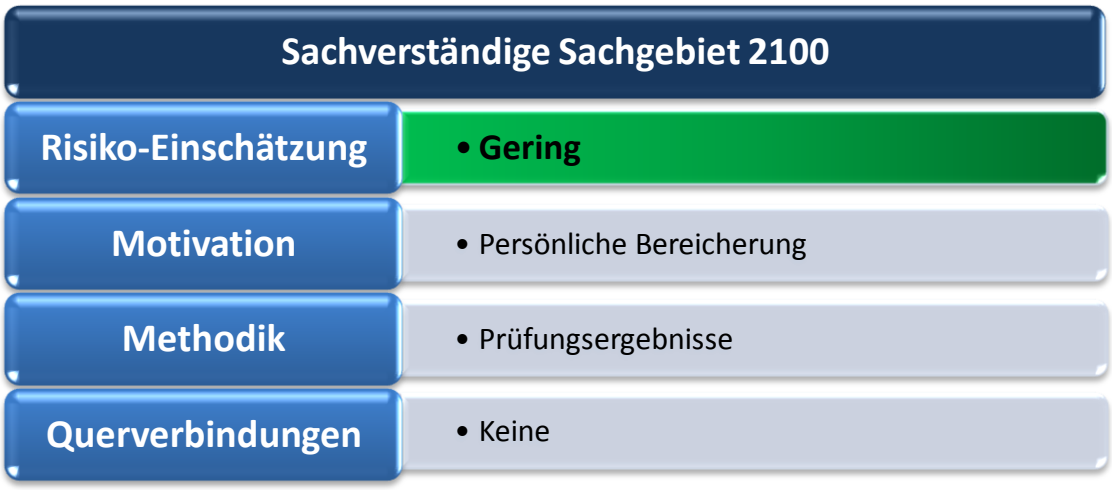



Bild 17: Risikoeinschätzung der Sachverständigen für Informationssysteme (branchenfremd)

### 7.6 Mitarbeiter des Herstellers

Programmierer, Hardwareentwickler und Mitarbeiter mit Zugang zu vertraulichen Informationen stellen aus zweifacher Sicht einen Risikofaktor dar: Einmal im direkten Auftrag (was bereits unter 7.2 Berücksichtigung findet) und einmal ohne Wissen ihres Arbeitgebers. Zum einen können sie mit Insider-Wissen, Hintertüren, ausgespähten Passwörtern etc. sehr viel direkten Schaden anrichten, aber auch durch Weitergabe von Informationen an Dritte indirekt Schaden verursachen.


Bild 18: Risikoeinschätzung der Herstellermitarbeiter

### 7.7 Mitarbeiter des Aufstellers

Mitarbeiter der Aufsteller unterliegen denselben Motiven wie die der Hersteller, wobei auch hier das direkte Befolgen von Aufstelleranweisungen separat unter 7.4 betrachtet wird. Die schädlichen Auswirkungen beschränken sich hauptsächlich auf den Aufsteller. Haben sie ihre Ursache in Insider-Wissen, welches auch auf Geräte anderer Aufsteller angewandt werden kann, wird dieser Risikofaktor unter 7.6 berücksichtigt.


Bild 19: Risikoeinschätzung der Aufstellermitarbeiter

### 7.8 Mitarbeiter der PTB

Mitarbeiter der PTB unterliegen denselben Motiven wie die der Hersteller und Aufsteller. Das direkte Befolgen von PTB-Anweisungen wird separat unter 7.2 betrachtet. Offensichtlich besteht hier die Möglichkeit, eine Bauartzulassung zu erteilen bzw. zu ihrer Erteilung beizutragen, indem Prüfergebnisse gefälscht werden oder einfach nur ungenügend geprüft wird. Obwohl der Kreis der in

Frage kommenden Mitarbeiter klein sein dürfte, sind die Auswirkungen einer gefälschten oder falschen Zulassung hoch. Solange der Ist-Prozess Aktivitäten dieser Art nicht verhindern kann, liegt hier ein erhebliches Potenzial für Missbrauch vor.

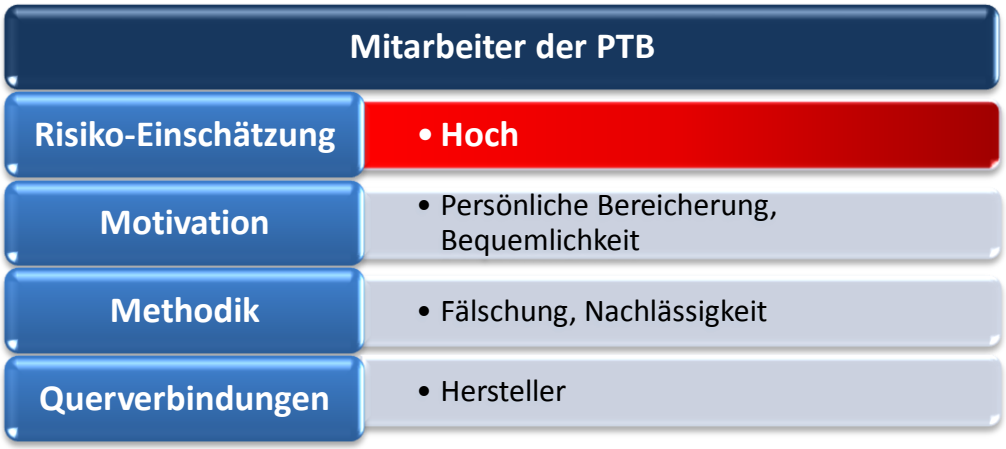



Bild 20: Risikoeinschätzung der PTB-Mitarbeiter

### 7.9 Auswirkung des Risikos (Impact)

Das offensichtlichste Risiko sind finanzielle Verluste am Gerät aufgrund von Manipulationen des Spielers. Aber auch fehlerhafte oder defekte Hard- und Software könnte zu finanziellen Verlusten am Gerät führen.

Weniger offensichtlich sind Sicherheitsrisiken, die zu einem Ausbleiben von Einnahmen führen, weil Spieler nicht an dem Gerät spielen können.

Ein Risiko besteht für Aufsteller, wenn manipulierte Geräte auf Dauer keinen Gewinn erwirtschaften bzw. zu viel oder zu wenig Gewinn für die Spieler ausschütten.

Mangelnde Nachweisbarkeit eines geregelten Betriebs ist für Hersteller, Aufsteller, Spieler und Behörden ein Risiko. Wenn ein Betrugsverdacht durch manipulierte Kontrollstreifen nur über statistische Auswertungen der zentralen Hersteller-EDV bestätigt oder entkräftet werden kann, ist eine sichere Aussage durch den Unsicherheitsfaktor Hersteller nicht vorhanden.

### 7.10 Risiko-Vektor

Interessant ist es noch, die Quellen bzw. Ausgangspunkte für die genannten Risiken etwas näher zu untersuchen. Während einige Quellen aufgrund des Prozessablaufs gegeben sind (z. B. die Überprüfung) und andere aufgrund mangelhafter Qualitätssicherung entstehen (Gerätezulassungen, die nicht ausreichend auf Gesetzeskonformität geprüft wurden), gibt es einen besonders auffälligen „Einstiegspunkt“ für die Ausbreitung vieler der genannten Risiken:

Ob Fehler bei der Zulassung, absichtliche Hintertürchen im eingespielten Objektcode, über Hardwareschnittstellen gesteuertes Geräteverhalten, Fehler in der Programmierung, ungewollter Zugang zum System – viele Risiken haben ihren Ursprung darin, dass die Kommunikation über die Hardwareschnittstellen das Auslösen und Umsetzen von denkbaren Sicherheitsrisiken erlaubt. Dies wird erschwert durch die Tatsache, dass Anwendung, Betriebssystem und Hardware vom Hersteller stammen und es keine Zusatzmaßnahmen im Ist-Prozess gibt, die einer solchen Konstellation die Einhaltung der Sicherheit aktiv aufzwingen könnten.

## 7.11 Beurteilung des Ist-Prozesses

Folgende Grafik beinhaltet die ermittelten, grundsätzlichen Risikofaktoren und deren Bewertung:


Bild 21: Risikofaktoren bezüglich Sicherheit

Dabei sei noch einmal auf die Zielsetzung (siehe 6.3 „Begriffsdefinition Sicherheit“) hingewiesen.

Die folgende Tabelle fasst die Einschätzung der Sicherheitsrisiken zusammen:

| | Gerät | PTB | Hersteller | Aufsteller | SV | Zugelassene Stellen | MA PTB | MA Hersteller | MA Aufsteller |
|---|---|---|---|---|---|---|---|---|---|
| **Umgehung der Sicherheit** | | | | | | | | | |
| **Bevorzugung eines Herstellers** | | | | | | | | | |
| **Unbeabsichtigte Fehler** | | | | | | | | | |
| **Persönliche Bereicherung** | | | | | | | | | |
| **Manipulationen durch Aufsteller** | | | | | | | | | |
| **Manipulationen durch Sachverständige** | | | | | | | | | |
| **Manipulationen durch zugelassene Stellen** | | | | | | | | | |
| ***Maximales Schadensrisiko*** | | | | | | | | | |

| Legende | | | |
|---|---|---|---|
| **Sehr hoch** | **Hoch** | **Mittel** | **Gering** |
| | | | |

Tabelle 3: Sicherheitsrisiken bezogen auf Beteiligte und deren Motive/Handlungen

Der aktuelle Ist-Prozess besitzt zwei besondere Schwachstellen, von denen in technischer Hinsicht die meisten Sicherheitsrisiken ausgehen:

- Software und Hardware des Geräts können problemlos manipuliert werden.
- Ein sicherer Nachweis dieser Manipulationen ist nicht gewährleistet.

Der Ist-Prozess beinhaltet eine aufwändige, doch letztlich sinnlose Prüfung, die keine Aussagekraft besitzt, aber durch die entstehenden Querverbindungen aus PTB, Hersteller und Prüfer ein erhebliches Sicherheitsrisiko einführt.

Der Ist-Prozess erlaubt aufgrund seiner Struktur keine Erhöhung der Sicherheit durch eine Verschärfung der zur Verfügung stehenden variablen Faktoren. Etwa der Einsatz kryptografisch sicherer Prüfsummen anstatt CRC32 würde trotzdem keine Aussage darüber erlauben, welche Software tatsächlich im Gerät betrieben wird bzw. wurde. Aus demselben Grund wäre auch ein Codereview oder Kompilieren des Sourcecodes als Schutzmaßnahme wirkungslos.

Die „Technische Richtlinie“ [ptb2] gibt den Herstellern Implementierungsdetails vor und überlässt deren Einhaltung den Herstellern, die einen Verwaltungsvertrag mit der PTB haben ([dbt1], Seite 3, letzter Satz). Dadurch wird der Ist-Prozess weder überprüfbar, noch lassen sich dessen Risiken reduzieren. Stattdessen wird „Security by Obscurity“ betrieben und die Verantwortung für die Einhaltung der Sicherheit in die Hände Beteiligter geben, die selbst oder deren Mitarbeiter eigene Interessen verfolgen. Dies bietet keinerlei Sicherheit vor Schäden.

Letztlich sind schon die Prüfkonfigurationen A, B und C für die Bauartzulassung derart konzipiert, dass Messungen über die Messschnittstelle jederzeit manipulierte Messwerte von den wichtigsten Kernkomponenten eines Spielgeräts erhalten könnten und somit keinerlei Nachweis über das zulässige Verhalten eines Bauartmusters möglich ist (6.1).

Grundsätzlich sollte der Prozess sämtliche Risiken in Bezug auf Bereicherung, Geschäftspraktiken und Konkurrenzdenken genauso ausschalten wie das Risiko für Diebstahl und Betrug. Dies kann der bestehende Ist-Prozess schon aus technischer Sicht nicht leisten.

Insbesondere mit dem Wortlaut des § 13 Abs. 1 Nr. 9 und 10 [spielv2] der Spielverordnung lässt sich der Ist-Prozess bzw. dessen Intention nicht in Einklang bringen:

9. *Das Spielgerät und seine Komponenten müssen der Funktion entsprechend nach Maßgabe des Standes der Technik zuverlässig und gegen Veränderungen gesichert gebaut sein.*

10. *Das Spielgerät muss so gebaut sein, dass die Übereinstimmung der Nachbaugeräte mit der zugelassenen Bauart überprüft werden kann.*

# 8 Grundsätzliche Überlegungen zu einem sicheren Prozesses

Grundvoraussetzung für einen sicheren Prozesses muss die eindeutige und nachweisliche Verifizierbarkeit des nachgebauten Geräts als exakte Funktionskopie des Bauartmusters sein. Ist diese gegeben, kann daraufhin das Gerät zuverlässig in einen zugelassenen Betrieb überführt werden. Dies muss ebenfalls in einer eindeutigen und nachweislichen Form geschehen.

## 8.1 Absicherung der Bauartzulassung

Die Zulassung durch die PTB anhand eines Bauartmusters umfasst sicherlich mehr Punkte als die in dieser Arbeit näher betrachtete Messschnittstelle. Diese sind aber nicht näher dokumentiert. Jedoch zeigen die unter 7.2 genannten Probleme indirekt, dass auch die Bauartzulassung als Ganzes offensichtliche Probleme in der Umsetzung aufweist und damit ein unsicheres Fundament für die eigentliche Geräteprüfung bildet.

Anhand der Messschnittstelle soll zumindest stellvertretend für die weiteren, nicht näher bekannten Zulassungsschritte eine sichere Alternative aufgezeigt werden:

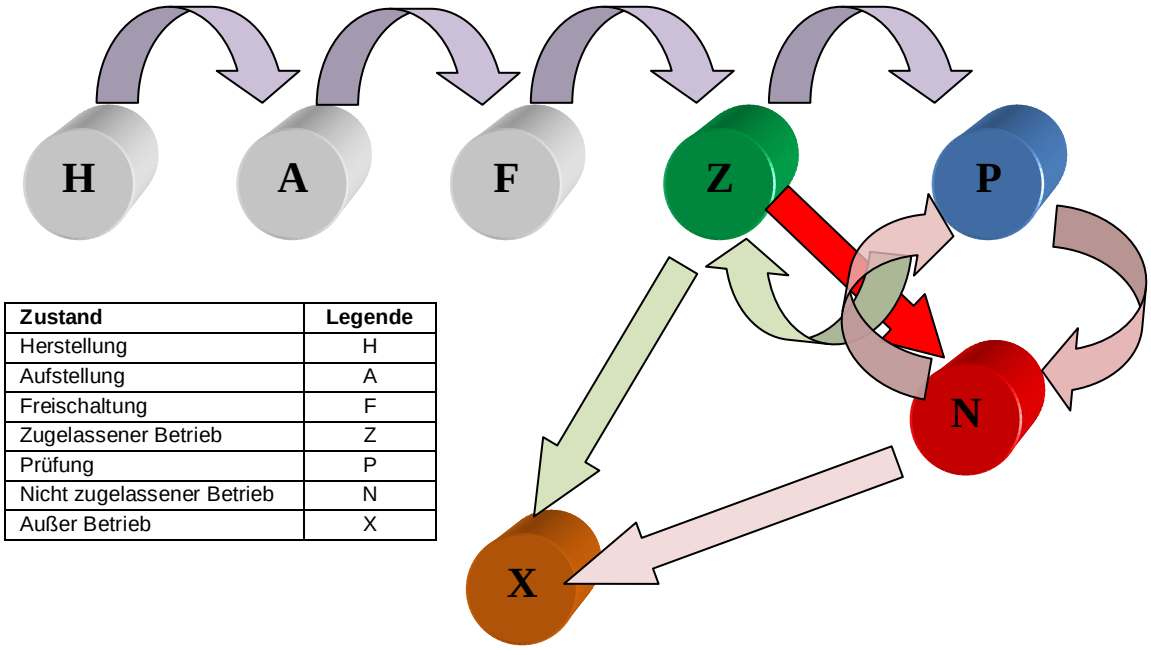
Das implementierte Prüfkonzept über die Messschnittstelle (Konfiguration A, B und C) ist nicht sicher, da dem Gerät mittels Protokoll mitgeteilt wird, dass und wie es geprüft werden soll. Aus diesem Grunde sind die so gewonnenen Erkenntnisse nicht verwertbar, da möglicherweise durch das Gerät manipuliert. Eine einfache Lösung wäre die Implementierung zweier Gigabit-LAN-Buchsen auf der Geräteplatine, die über eine Brücke miteinander verbunden sind. Sowohl das Monitoring (Prüfkonfiguration C) wie auch die Prüfung der Kontrolleinrichtung (A) und der Spielsteuerung (B) wären durch das Einschleifen eines PC als „Transparent Bridge“ für das Geldspielgerät unbemerkt zu bewerkstelligen. Da diese Prüfkonfigurationen nur der PTB zugänglich zu machen sind, würde die Verschlüsselung des Datenverkehrs nicht nur die bestehende, von der PTB geforderte einfache Passwortabfrage überflüssig machen, sondern grundsätzlich die Sicherheit dieser Schnittstelle auf ein vernünftiges Maß erhöhen. In der Praxis würde ein PC bei ausgeschaltetem Geldspielgerät als „Man in the Middle“ eingeschleift werden und mit einer Netzwerküberwachungssoftware wie beispielsweise Wireshark ausgestattet sein, um den Netzwerkverkehr zu protokollieren. Nur wenn der kryptografische Schlüssel bekannt ist, ließe sich der mitgehörte Datenverkehr auch dekodieren und manipulieren.

Allerdings sind diese Maßnahmen nur mittelfristig umsetzbar, da sie neue Hardware vom Hersteller verlangen.

Ein weiterer Aspekt ist das völlige Fehlen eines Qualitätssicherungskonzepts zur Überprüfung und Korrektur einer einmal ausgesprochenen Zulassung. Es fehlt ein Qualitätsmanagement durch die PTB, beispielsweise um alle Beteiligten zeitnah, nachweislich und effektiv darüber zu informieren, ob es Geräte mit falschen Checksummen oder nicht zulässigem Verhalten gibt, ob Nachträge zu vorhandenen Zulassungen oder neue Zulassungen ausgestellt wurden etc.

Insgesamt ist bereits aus diesen wenigen Beispielen ersichtlich, dass die Bauartzulassung selbst sehr fehleranfällig sein muss. Hinzu kommen noch extrem kritische Zulassungsinhalte, die in dieser Arbeit gar nicht berücksichtigt werden Etwa die nachweisliche Überprüfung des statistischen Verhaltens eines Baumusters bei den Glücksspielen, dessen Bewertung ausgesprochenes mathematisches und statistisches Fachwissen erfordert.

## 8.2 Vereinfachung des Prozessablaufs




| Zustand | Legende |
|---|---|
| Herstellung | H |
| Aufstellung | A |
| Freischaltung | F |
| Zugelassener Betrieb | Z |
| Prüfung | P |
| Nicht zugelassener Betrieb | N |
| Außer Betrieb | X |

Bild 22: Zustandsdiagramm der Ist-Prüfung

Durch eine einfache Verlagerung der Prüfung an die Stelle der Freischaltung nach der Aufstellung wird die Möglichkeit für einen sicheren Prüfprozess geschaffen. Zusätzlich entsteht ein vereinfachtes Prüfverfahren, welches nicht mehr wiederholt werden müsste, solange das Gerät im zugelassenen Betrieb verbleibt.

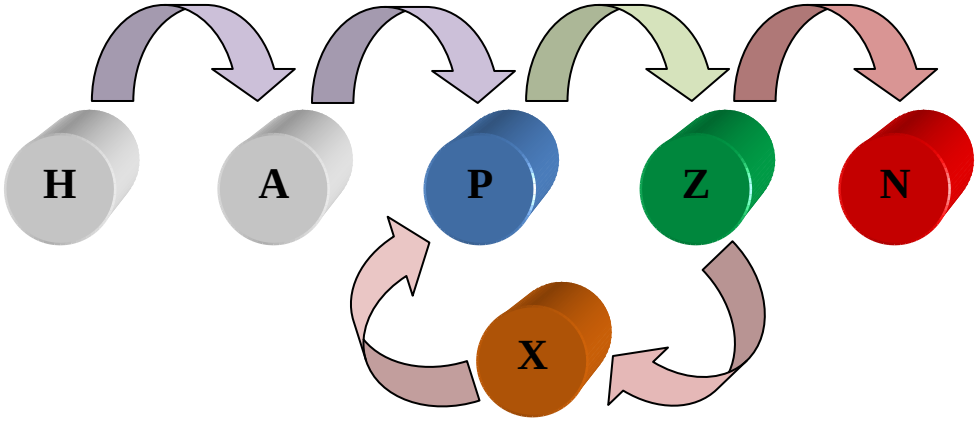



Bild 23: Zustandsdiagramm des vereinfachten Soll-Prozesses

Die bisherige Praxis, ein fertiges Gerät, bestehend aus Hard- und Software, herzustellen und auszuliefern und vom Aufsteller freischalten zu lassen, bietet Angriffspunkte für die Sicherheit des zugelassenen Betriebs:

- Es befinden sich bereits eine Anwendungssoftware und ein Betriebssystem im Gerät.
- Von der Software unterstützte Hardwareschnittstellen sind damit prinzipiell einsatzfähig.
- Das Betriebssystem bietet Möglichkeiten, Zusatzanwendungen auszuführen.
- Lediglich eine fehlende PIN-Karte verhindert den Betrieb des Geräts.

Deutlich sicherer wären die Herstellung, Auslieferung und Aufstellung des Geräts ohne Software (Anwendung und Betriebssystem). Damit könnte ein fachlich qualifizierter Prüfer grundsätzlich die Software selbst installieren und verifizieren.

### 8.3 Überlegungen zur Einhaltung des zugelassenen Betriebszustands

Damit bieten sich alle Möglichkeiten moderner kryptografischer Verfahren an, um die Kombination aus Soft- und Hardware eindeutig zu signieren und abgerufene oder ausgegebene Daten eindeutig und nachvollziehbar einem Gerät und seiner Software zuzuordnen.

Mit zusätzlichen auf Software basierenden Maßnahmen kann dieser zugelassene Betriebszustand so sichergestellt werden, dass ein Angreifer nur mit unverhältnismäßig hohem Aufwand diesen manipulieren kann, ohne dass Manipulationsversuche vom Gerät erkannt werden.

### 8.4 Überlegungen zur Außerbetriebnahme des Geräts

Manipulationsversuche sollten damit enden, dass das Gerät automatisch in einen Zustand versetzt wird, der keinen weiteren Betrieb zulässt. Eine Umgehung wäre nur mit unverhältnismäßig hohem Aufwand verbunden und mit einer damit einhergehenden direkten oder indirekten Nachweisbarkeit des unzulässigen Betriebs.

Insbesondere der konsequente Einsatz von Signaturen für alle ausgegebenen Daten würde ein einfaches Aufsetzen neuer Software nachträglich nachvollziehbar machen.

### 8.5 Auswirkung auf die Freischaltung

Das sichere Verfahren sieht keine Freischaltung über Hersteller-PIN mittels Kartenleser vor, womit diese Schnittstelle überflüssig wird und das damit verbundene Risiko [dbt1] wegfällt.

### 8.6 Auswirkung auf die Prüfung

Der vereinfachte Soll-Prozess macht die in § 7 SpielV alle 24 Monate geforderten Prüfungen prinzipiell überflüssig. Solange § 7 SpielV diese jedoch vorsieht, kann deren Durchführung mittels kryptografischer Verfahren drastisch vereinfacht und in deutlich kürzeren Prüfzeiten vollzogen werden.

Der Prüfer kann mittels eines einfachen Challenge-/Response-Verfahrens die Gültigkeit des aktiven Binärcodes prüfen. Ein solcher Vorgang wäre in wenigen Minuten und ohne Ziehen von EPROMs oder Auslesen von Binärcode realisierbar, würde das Risiko einer Geräteschädigung minimieren und wäre auch mit Sachverständigen des Sachgebiets 530 und Prüfern von zugelassenen Stellen realisierbar.

Das Restrisiko, dass ein Prüfer ein Gerät mit falschem Response-Verhalten zulässt, wäre durch die zentrale Abgabe des Prüfberichts unter Angabe der benutzten und erhaltenen Werte nachweisbar.

# 9 Kryptografische Grundlagen

Im Folgenden werden grundlegende kryptografische Verfahren vorgestellt, die als Grundvoraussetzung für einen sicheren Soll-Prozess betrachtet werden dürfen.

## 9.1 Symmetrische Verfahren

Symmetrische Verfahren erzeugen für den Inhaber eines Geheimnisses einen Schlüssel, welcher für die Ver- und Entschlüsselung benutzt wird. Symmetrische Verfahren verlangen eine Schlüsselübergabe an den Nachrichtenempfänger, womit ein Sicherheitsrisiko entstehen kann, je nachdem, unter welchen Bedingungen die Schlüsselübergabe erfolgen muss. Um dieses Sicherheitsrisiko zu senken und einen Schlüsseltausch über unsichere Kanäle bewerkstelligen zu können, wird auf kryptografische Schlüsseltauschverfahren wie „Diffie-Hellman“ zurückgegriffen.

Vorteil der symmetrischen Verfahren ist deren schnelle Berechnung.

Über symmetrische Kryptoverfahren lassen sich Nachrichten verschlüsseln und entschlüsseln.

Momentan gilt AES (Advanced Encryption Standard) als sicher.

## 9.2 Asymmetrische Verfahren

Asymmetrische kryptografische Verfahren erzeugen für einen Inhaber ein Schlüsselpaar, bestehend aus einem privaten Schlüssel und einem öffentlichen Schlüssel. Der private Schlüssel bleibt im Besitz des Inhabers, wogegen der öffentliche Schlüssel an Dritte herausgegeben bzw. diesen zugänglich gemacht wird. In der Regel wird der private Schlüssel mittels eines Geheimnisträgers aufbewahrt wie etwa Chipkarte o. Ä. und darf Dritten nicht zugänglich sein.

Nachteil asymmetrischer Verfahren ist der dafür benötigte Rechenaufwand.

Über asymmetrische Kryptoverfahren lassen sich Nachrichten verschlüsseln/entschlüsseln und Nachrichten signieren/verifizieren.

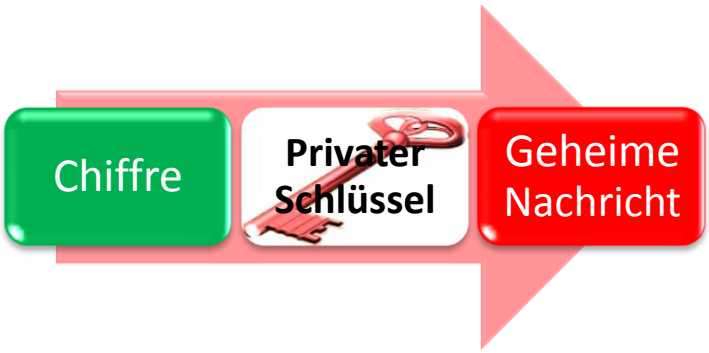
Momentan gilt der „Elliptic Curve“-Algorithmus als ein sicherer asymmetrischer Standard.

### 9.3 Verschlüsseln und Entschlüsseln

Prinzipiell trifft folgende Beschreibung auch für das Verschlüsseln und Entschlüsseln mit symmetrischen Verfahren zu, allerdings gibt es dabei keinen öffentlichen Schlüssel, sondern nur den privaten Schlüssel, mit dem sowohl kodiert wie dekodiert wird.

Damit ein Absender (Dritter) eine Nachricht verschlüsselt an einen Empfänger (Inhaber) übermitteln kann, benutzt der Absender den öffentlichen Kodierschlüssel $ECK_I$ des Empfängers, um damit seine Nachricht zu verschlüsseln (enkodieren).


Der Empfänger, welcher gleichzeitig der Inhaber des Schlüsselpaares ist, benutzt seinen geheimen privaten Dekodierschlüssel $DCK_I$, um die Nachricht zu entschlüsseln (dekodieren).

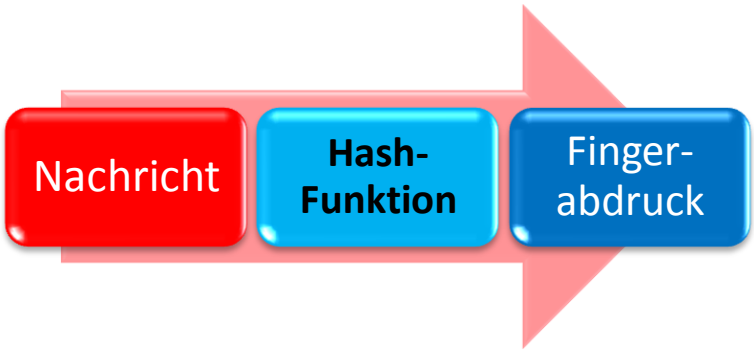



Der öffentliche Schlüssel ist lediglich für das Verschlüsseln, jedoch nicht für das Entschlüsseln geeignet.

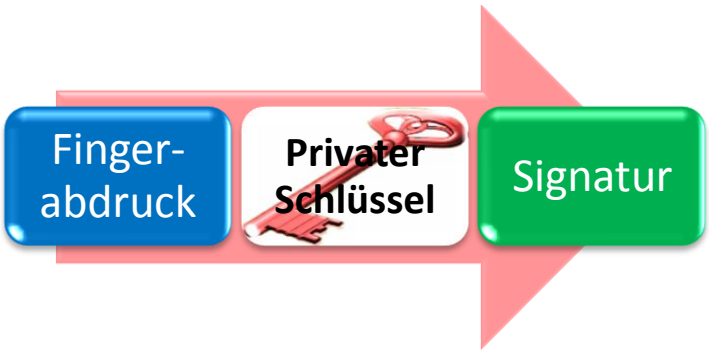
### 9.4 Signaturen

Eine Signatur dient dazu festzustellen, ob eine übermittelte Nachricht von einem bestimmten Absender stammt und nicht manipuliert wurde. Der Absender ist in diesem Falle der Inhaber des Schlüsselpaares und der Empfänger ein Dritter mit Zugang zum öffentlichen Schlüssel des Absenders - also umgekehrt zu 9.3.

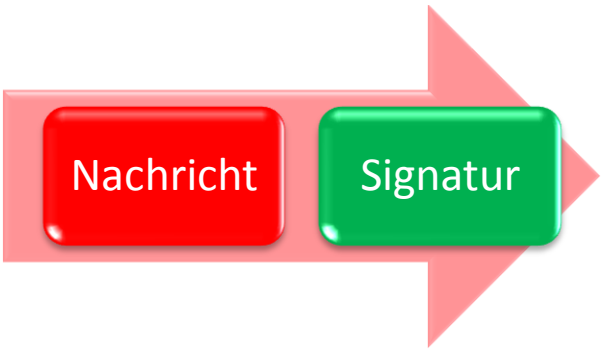
Aus einer Nachricht wird vom Absender (Inhaber) mit einer Hash-Funktion ein Hash-Wert erzeugt (Fingerabdruck). Die Hash-Funktion ist sowohl Absender wie Empfänger bekannt:



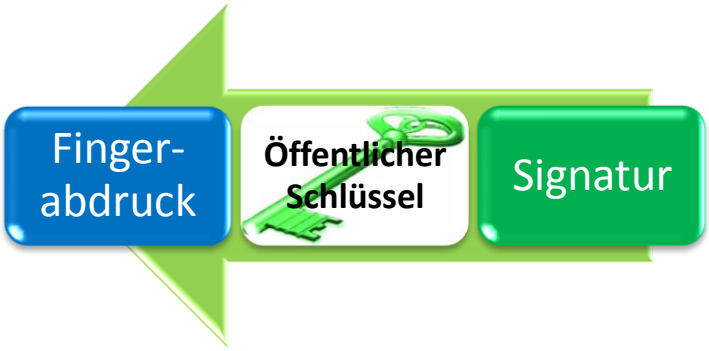

Mit dem privaten Signaturschlüssel $ESK_I$ werden der Hash-Wert und ggf. Zusatzinfos vom Absender (Inhaber) als Signatur zu einem Message Digest verschlüsselt (enkodiert):



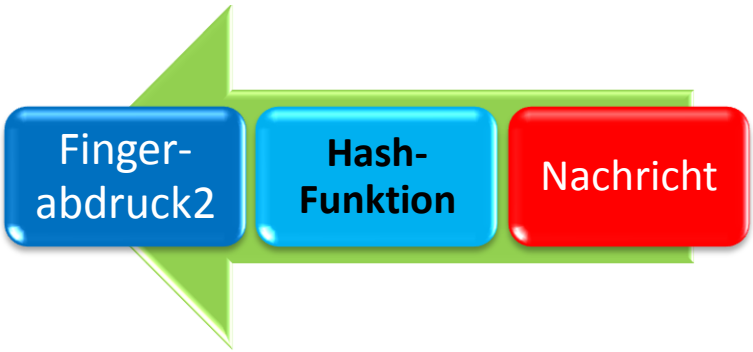

Der Empfänger erhält ein Paket aus Nachricht und Signatur zugestellt:



Mit dem öffentlichen Signaturschlüssel $DSK_I$ des Absenders (Inhaber) wird die übermittelte Signatur durch den Empfänger (Dritter) entschlüsselt (dekodiert):




Der Empfänger erzeugt aus der übermittelten Nachricht ebenfalls einen Hash-Wert:




Zuletzt vergleicht er diesen mit dem Hash-Wert aus der Signatur:


Im Gegensatz zur Verschlüsselung/Entschlüsselung, wo der öffentliche Schlüssel zum Verschlüsseln einer geheimen Nachricht durch einen Dritten verwendet wird, benutzt der Dritte bei der Signatur den öffentliche Schlüssel zur Überprüfung einer – wenn auch bereits bekannten – Nachricht. Natürlich ist hierbei sicherzustellen, dass der verwendete öffentliche Schlüssel zur Bestätigung der Signatur auch vom tatsächlichen Absender stammt. Dies kann z. B. über Trust Center oder Rückfragen sichergestellt werden.

Die Signatur dient gleichzeitig zur Überprüfung von Integrität, Authentifizierung und Authentizität einer Nachricht.

## 9.5 Hash-Funktionen

Kryptografische Hash-Funktionen sind sogenannte Einwegfunktionen, die aus einer u. U. umfangreichen Nachricht (wie etwa ein Binärcode) eine Prüfsumme (Fingerabdruck) berechnen. Die Prüfsumme hat zumeist eine bestimmte Länge und ist damit normalerweise sehr viel kleiner als die Nachricht, aus der sie erzeugt wurde.

Wichtig sind folgende Eigenschaften bei einer Hash-Funktion:

- **Einwegfunktion (preimage resistant):** Aus dem Ergebnis lässt sich nicht auf die ursprüngliche Nachricht schließen, bzw. aus einem gegebenen Ausgabewert h(x) = y kann praktisch nicht auf x geschlossen werden.
- **Schwach kollisionsfrei (2nd preimage resistant):** Wenn es zu einem gegebenen x praktisch unmöglich ist, ein davon verschiedenes x‘ mit h(x) = h(x‘) zu finden.
- **Stark kollisionsfrei (collision resistant):** Wenn es praktisch unmöglich ist, ein x und ein davon verschiedenes x‘ zu finden mit h(x) = h(x‘).

## 9.6 CRC32

Der CRC32-Algorithmus - „Cyclic Redundancy Check“ - erzeugt eine 32 Bit lange digitale Checksumme. Daraus können $2^{32}$ unterschiedliche Fingerabdrücke erzeugt werden.

Allerdings wurde das Verfahren entwickelt, um Unterschiede zwischen einem übertragenen Datenstrom und dem Original festzustellen. Unterschiedliche Checksummen bedeuten mit hundertprozentiger Sicherheit, dass es zu einem Übertragungsfehler gekommen ist.

Sicherheit im kryptografischen Sinne ist deshalb nicht gegeben, weil es relativ einfach ist, zwei unterschiedliche Datenströme zu erzeugen, welche dieselbe Checksumme besitzen.

Die Wahrscheinlichkeit, dass sich ein Datenstrom A bei der Übertragung so verändert, dass er als Datenstrom B erscheint, ist für den gedachten Einsatzzweck von CRC32 ausreichend unwahrscheinlich.

Der Einsatz von CRC32 führt diesen Unsicherheitsfaktor unnötigerweise und entgegen dem Stand der Technik bei der Überprüfung von Geldspielgeräten ein und lässt damit grundsätzlich zu, dass unterschiedliche Binärcodedateien mit gleicher Checksumme entwickelt und unentdeckt in Geldspielgeräten zum Einsatz kommen könnten.

# 10 Kryptografisches Absichern der Zulassung

Wendet man die in 9 gezeigten kryptografischen Grundlagen auf die einzelnen Teile des in 8.2 dargestellten vereinfachten Prozesses an, ergeben sich die Voraussetzungen für einen sichereren Soll-Prozess. Dieser verlangt von Hersteller, zulassender Stelle und Prüfer jeweils ein eigenes asymmetrisches Schlüsselpaar, um eine konsequente Signierung umsetzen zu können. Aus sicherheitstechnischen Erwägungen heraus sollten die öffentlichen Schlüssel durch eine offizielle Zertifizierungsstelle signiert werden.

## 10.1 Abgesicherte Softwareerstellung

Das Zulassungsverfahren ist im Soll-Prozess besonders kritisch. Offensichtlicher Ansatzpunkt für eine Erhöhung der Sicherheit ist der Einsatz von Signaturen. Die PTB darf nur vom Hersteller korrekt signierten Sourcecode annehmen. Der von der PTB erzeugte Objektcode muss von der PTB signiert werden.

Das Verfahren sollte ausschließlich auf öffentliche Schlüssel zurückgreifen, die unter besonderen Sicherheitsmaßnahmen veröffentlicht wurden. Damit wird verhindert, dass aufgrund eines vom Absender mitgelieferten öffentlichen Verifizierungsschlüssels eine falsche Signatur (z. B. von einem Mitarbeiter stammend) verifiziert wird.

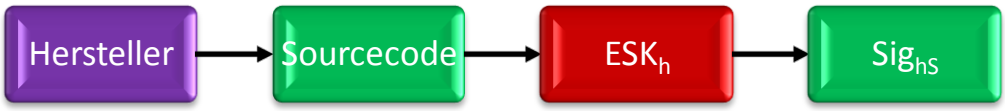



Bild 24: Durch den Hersteller signierter Sourcecode

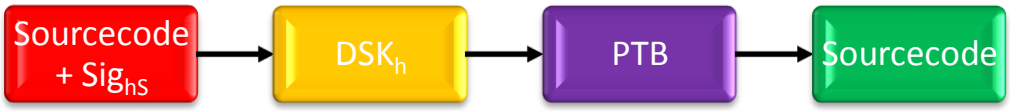



Bild 25: Abgesicherte Sourcecode-Übernahme durch die PTB


Bild 26: Signierte Objektcode-Erzeugung durch die PTB

Bedeutung kommt an dieser Stelle auch einem Code-Review zu, dessen Qualität darüber bestimmt, ob es einem Hersteller trotzdem möglich gemacht wird, Software mit unerlaubten Zusatzfunktionen weiterzugeben, die sich letztlich im Objektcode wiederfinden werden. Dies kann durch aktive Sicherheitsmaßnahmen noch bis zu einem bestimmten Grad erkannt und abgefangen werden.

## 10.2 Abgesicherte Betriebssystemübernahme

Im Unterschied zum Sourcecode erfolgt beim Betriebssystem keine Kompilierung, sondern die Übergabe als signierte Image-Datei.

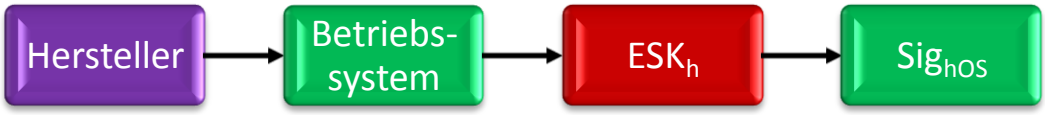



Bild 27: Signiertes Betriebssystem durch den Hersteller

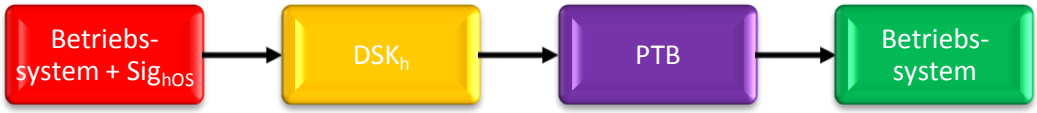



Bild 28: Abgesicherte Betriebssystem-Übernahme durch die PTB

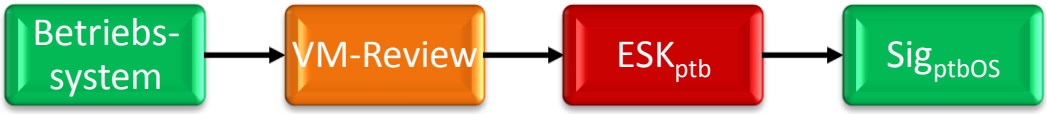



Bild 29: Signiertes Betriebssystem durch die PTB

Ein VM-Review könnte eingeführt werden, um das Betriebssystem in einer Virtuellen Maschine auf eine unsichere Konfiguration hin zu überprüfen.

# 11 Praktischer Lösungsansatz

Wie bereits in 7.11 erwähnt, müssen zwei grundlegende Schwachstellen des Ist-Prozesses behoben werden bzw. muss sichergestellt sein, dass diese nur mit unzumutbar hohem Aufwand ausgenutzt werden können:

- Software und Hardware des Geräts können problemlos manipuliert werden.
- Ein sicherer Nachweis dieser Manipulationen ist nicht gewährleistet.

Der Ist-Prozess arbeitet bereits mit einem Checksummen-Verfahren, welches jedoch hinsichtlich der Sicherheit als ungeeignet eingestuft werden muss. Auch wenn die Schwächen des aktuell praktizierten CRC32-Verfahrens durch Anwendung einer kryptografischen Hash-Funktion vermieden werden würden, ist es mit dem Ist-Prozess nicht möglich, die obigen Schwachstellen zu beheben.

Wird jedoch der Binärcode der Anwendung eindeutig der Gerätehardware zugeordnet, kann auch sichergestellt werden, dass ein installierter Binärcode nur auf diesem Gerät betrieben werden kann, womit Signaturen als Sicherheitsmerkmal für den Soll-Prozess sinnvoll eingesetzt werden können.

Um die Umgebung für ein sicheres Verfahren herzustellen, muss auf jeden Fall die Manipulation von Hard- und Software weitestgehend an einen Nachweis dieser Manipulation gekoppelt werden. Jede erfolgreiche Manipulation – die schon selbst nur mit unverhältnismäßig hohem Aufwand durch einen Angreifer möglich sein darf – muss zu einem nachträglichen eindeutigen Nachweis der Manipulation führen, dessen Umgehung einen noch höheren Aufwand von einem Angreifer verlangt.

Dazu bedarf es im laufenden Betrieb einer Kombination aus drei Komponenten, die im Zusammenspiel den Aufwand für einen erfolgreichen Angriff auf die Sicherheit unverhältnismäßig hoch werden lassen:

- Sicherstellung kryptografisch abgesicherter Ein-/Ausgabe
- Ein sicherer Geheimnisträger
- Ein aktiver Sicherheitsmechanismus, um auf Änderungen an der installierten Gerätekonstellation zu reagieren.

## 11.1 Kryptografische Ein- und Ausgabe

Sämtliche Eingaben über Hardwareschnittstellen müssen nach einem standardisierten Protokoll erfolgen, mittels des öffentlichen Schlüssels des Geräts $ECK_G$ verschlüsselt.

Sämtliche Ausgaben des Soll-Prozesses an Hardwareschnittstellen müssen mit einem Zeitstempel und einem fortlaufenden Zähler versehen werden. Diese Informationen werden signiert, damit Dritte im Nachhinein die Integrität und Authentizität der Daten nachweisen und das Gerät selbst identifizieren können.

Insbesondere die Ausgaben und Ausdrucke von Abrechnungsdaten müssen Signaturen aufweisen.

Die Signatur basiert auf einem privaten Signaturschlüssel des Geräts $ESK_G$, welcher eindeutig der Kombination aus Gerätehard- und –software zugeordnet ist. Der private Signaturschlüssel wird in einem sicheren Geheimnisträger aufbewahrt. Erfolgt die Verarbeitung ausschließlich durch eine herstellerunabhängige Softwareschnittstelle, kann diese unerlaubte Befehlsfolgen abfangen.

## 11.2 Geheimnisträger Dongle

Um kryptografische Verfahren umsetzen zu können, bedarf es eines geeigneten Geheimnisträgers, der den privaten Signaturschlüssel $ESK_G$ und privaten Dekodierschlüssel $DCK_G$ des Geräts sicher aufzubewahrt. Hierfür sind beispielsweise Dongle geeignet.

Aufgrund ihrer vielfältigen Bauformen sind sie an jeder Herstellerhardware anbringbar, womit der Soll-Prozess keinerlei Änderungen in Konstruktion oder Herstellung der Gerätehardware verlangt. Gleichzeitig sind entsprechend konstruierte Dongle kryptografisch sicher in dem Sinne, dass deren gespeichertes Geheimnis nur unter unverhältnismäßig hohem Aufwand in Erfahrung zu bringen ist (nach heutigem Wissenstand) und sie bereits Hardware für grundlegende kryptografische Aufgaben aufweisen.

Das Ziel besteht zunächst darin, einen Dongle mit geeigneten privaten und öffentlichen Schlüsseln für Chiffrieren/Dechiffrieren und Signieren/Verifizieren zu versehen.

Die öffentlichen Schlüssel sollen auslesbar sein.

Die privaten Schlüssel dürfen nur unter unverhältnismäßig hohem Aufwand auslesbar sein.

## 11.3 Aktiver Sicherheitsmechanismus

Gerätehardware die im Wesentlichen einem PC gleicht, besitzt als unvermeidbaren Sicherheitsschwachpunkt den einfachen Austausch der Anwendungssoftware und/oder des Betriebssystems, wodurch das System nach Gutdünken verändert werden kann. Ohne spezielle Lösungen wie etwa auf Basis von Trusted Computing zu fordern, kann der Soll-Prozess nur bis zu einem bestimmten Grad verhindern, dass die Gerätehardware nicht so eingesetzt wird, wie es der zugelassene Betrieb erfordert.

Der Einsatz eines Geheimnisträgers alleine bietet keine Lösung, da zwar Start und Ausführung einer Anwendung überprüft werden können, jedoch nicht Start und Ausführung einer Software, die unabhängig vom Geheimnisträger agiert.

Deshalb müssen zusätzlich aktive Sicherheitsmaßnahmen implementiert werden, die nach der Freischaltung verhindern (bzw. nur mit unverhältnismäßig hohem Aufwand zulassen), dass ein Gerät durch Manipulation der Software sich so verhalten kann, wie ein zugelassenes Gerät. Kommt es zu einem Manipulationsversuch, soll das Gerät außer Betrieb gesetzt werden und keine neuerliche Inbetriebnahme in einem zugelassenen Betriebszustand möglich sein – außer durch einen Prüfer.

Damit wären folgende Sicherheitsrisiken zu vermeiden bzw. eindeutig nachweisbar:

- Manipulationen an Hard- und Software durch den Hersteller vor der Aufstellung
- Manipulationen an Hard- und Software durch den Hersteller nach der Aufstellung
- Nachträgliche Manipulationen an Hard- und Software durch Mitarbeiter des Herstellers
- Nachträgliche Manipulationen an Hard- und Software durch Mitarbeiter der PTB
- Nachträgliche Manipulationen an Hard- und Software durch den Aufsteller
- Manipulationen durch den Aufsteller
- Manipulationen durch Mitarbeiter des Aufstellers
- Manipulationen durch Sachverständige beim zweijährigen Prüfungsverfahren
- Manipulationen durch zugelassene Stellen beim zweijährigen Prüfungsverfahren

# 12 Konzeption des aktiven Sicherheitsmechanismus

Der aktive Sicherheitsmechanismus muss zum einen soweit wie möglich sicherstellen, dass nur die Software im Gerät arbeiten kann, die dafür vorgesehen ist, ohne dafür besondere Schutzmaßnahmen zu verlangen, die nur mit spezieller Hardware realisierbar wären.

Zum anderen müssen mögliche Angriffspunkte auf das laufende Gerät abgesichert werden, um die Ausführung einer möglicherweise vorhandenen unerwünschten Funktionalität zu verhindern.

Die Anforderungen im Detail:

- Es sollte ein nachträglich einzubringender Mechanismus sein, unabhängig von dem in das Gerät eingespielten Binärcode (Anwendung und Betriebssystem).
- Es sollte die vollständige Kontrolle über die Ein- und Ausgabeschnittstellen des Geräts zur Abschottung aller Schnittstellen ermöglicht werden (Schutzmantel).
- Es sollte ein Angriff auf die Gerätesicherheit erkannt werden, was in der Folge zu einer aktiven Außerbetriebnahme führen muss (Wächter).
- Es sollte bei einem erfolgreichen Angriff nicht möglich sein, den Mechanismus für kryptografische Aufgaben zu missbrauchen.

Die geforderten Eigenschaften ähneln den heute bekannten Rootkits und Viren. Durch eine gezielte Infektion der vom Hersteller gelieferten Software kann diese ohne aufwändige Kontrolle des Sourcecode nachträglich und ohne Einflussnahme des Herstellers abgesichert werden.

## 12.1 Aufgaben des „Schutzmantels“

Der Schutzmantel hat folgende Aufgaben zu erfüllen:

- Absicherung sämtlicher Hardwareschnittstellen gegen eine freie Kommunikation von außen nach innen und umgekehrt
- Überwachung der erlaubten Protokolle und Steuerzeichen
- Automatisches Signieren aller Ausgaben
- Automatisches Dekodieren aller Eingaben
- Automatisches Kodieren entsprechender Ausgaben
- Automatisches Verifizieren aller Eingaben
- Insbesondere Absicherung der Dongle-Kommunikation
- Außerbetriebnahme des Geräts bei erkannten Angriffen

Anstatt Sourcecode oder Betriebssystemcode auf mögliche Sicherheitslücken – gewollt oder ungewollt – zu prüfen bzw. wie beim Ist-Prozess dieses Risiko einfach hinzunehmen, wäre der Schutzmantel ein nachträglicher Absicherungsmechanismus für das Betriebssystem.


Bild 30: Einbindung des Schutzmantels in das Gerät

Die bestehende Gerätekommunikation soll bereits im Ist-Prozess bestimmten Protokollen oder Steuerzeichen folgen (siehe [ptb2], Seite 36 ff). Das Risiko besteht natürlich darin, dass noch weitere Protokolle oder Steuerzeichen zum Einsatz kommen könnten, die nicht vorgesehen sind. Der Schutzmantel kann diese Art nicht vorgesehener Kommunikation ausfiltern. Damit wären nicht nur „Brute Force"-Attacken über LAN-Schnittstellen zum Suchen möglicher Zugänge, sondern auch von Mitarbeitern eingearbeitete Zusatzfunktionen und Ähnliches, effektiv und ohne Dazutun des Herstellers, wirkungslos.

Schon aus Gründen der Sicherheit, aber auch aus wirtschaftlichen Erwägungen heraus, bietet eine Umleitung der Kommunikation die effektivste Methode, um ausgehende Daten zusätzlich zu signieren, damit vom Empfänger der Daten jederzeit anhand des öffentlichen Signaturschlüssels die Echtheit der Nachricht verifiziert werden kann.

Als weiteren Schutz akzeptiert der Schutzmantel eingehende Daten nur verschlüsselt und signiert.

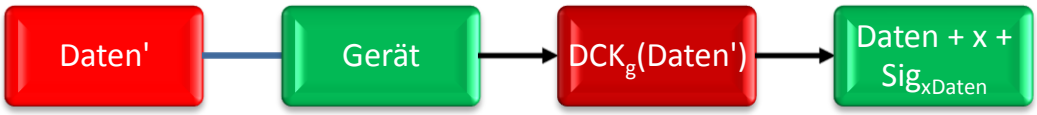



Bild 31: Entschlüsseln eingehender Daten


Bild 32: Verifizieren eingegangener Daten

D.h., der eingehende Datenstrom *Daten'* muss mit dem öffentlichen Chiffrierschlüssel $ECK_G$ des Geräts verschlüsselt worden sein, um überhaupt mit dem Gerät kommunizieren zu können. Dieser verschlüsselte Datenstrom wird mit dem privaten Dechiffrierschlüssel $DCK_G$ des Geräts entschlüsselt, welcher nur auf dem Geheimnisträger Dongle existiert.

Entsprechend einem Protokoll liegen dann sowohl die eigentlichen *Daten*, deren Urheber *x* und dessen Signatur für die Daten $Sig_{xDaten}$ vor. Als Urheber kommen somit lediglich Hersteller, PTB oder Sachverständige in Frage.

Da der Dongle über eine Hardwareschnittstelle angesprochen werden muss, kann die Kommunikation mit dem Dongle zusätzlich abgesichert werden. In der Regel werden Dongle mit einer Herstellersoftware angesprochen, die selbst verschlüsselt mit dem Dongle kommuniziert. Der Schutzmantel kann die Kommunikation dieser Software zum Dongle mit seiner eigenen Kommunikation zur Dongle-Software kontrollieren und damit eine unerlaubte Dongle-Kommunikation abfangen.

## 12.2 Aufgaben des Wächterprogramms

Der Schutzmantel ist in der Lage die Ein- und Ausgabe des Betriebssystems zu verändern. Er erkennt jedoch nicht, ob die korrekte Anwendungssoftware läuft oder das Gerät kompromittiert ist. Auch ist das Betriebssystem nicht in der Lage zu erkennen, ob eine Hardwareschnittstelle von einer Anwendung direkt angesprochen wird.

Um diese Aufgaben zu bewerkstelligen dient ein Wächterprogramm:

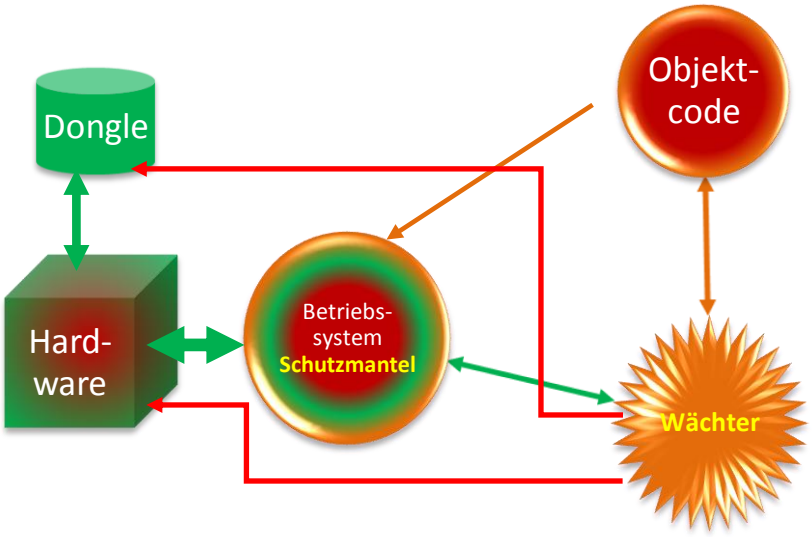



Bild 33: Aktive Komponenten im abgesicherten Betrieb

Vor dem Einspielen von Betriebssystem und Objektcode werden diese mit Schutzmantel und Wächterprogramm „infiziert“ und dadurch beim ersten Start im Gerät von letzteren modifiziert. Nach diesem Zeitpunkt neu hinzukommende Anwendungen oder Prozesse werden vom Wächterprogramm korrumpiert und beendet.

Die Aufgaben des Wächterprogramms im Einzelnen:

- Vermehrung auf maximal *n* Instanzen
- Regelmäßiges Überprüfen auf Vorhandensein des Dongle
- Regelmäßiges Überprüfen auf Vorhandensein des (modifizierten) Objektcodes
- Regelmäßiges Überprüfen auf Vorhandensein des Schutzmantels
- Regelmäßige direkte Überwachung der Hardwareschnittstellen
- Außerbetriebnahme des Geräts bei erkannten Angriffen

Fehlen Dongle, Schutzmantel oder die modifizierte Anwendung, wird das Gerät außer Betrieb gesetzt.

## 13 Anforderungen an die Freischaltung

Das Einführen eines aktiven Sicherheitsmechanismus in Form eines Schutzmantels und eines Wächters hat insofern Auswirkungen auf die Freischaltung, dass diese die notwendigen Informationen zur Einhaltung des aktiven Sicherheitsmechanismus liefern muss.

Für die Freischaltung bietet sich eine automatisierte Lösung an, welche gleichzeitig die wichtigen Daten in einem elektronischen Prüfbericht für eine zentrale Hinterlegung zusammenfasst. Die Überprüfung des Objektcodes und des Betriebssystems (Image-Datei) sollte auch hier nur mit öffentlichen Signaturschlüsseln erfolgen, die nicht mit dem Objektcode bzw. Betriebssystem-Image und deren Signaturen mitgeliefert werden, ähnlich wie bereits in 10 beschrieben.

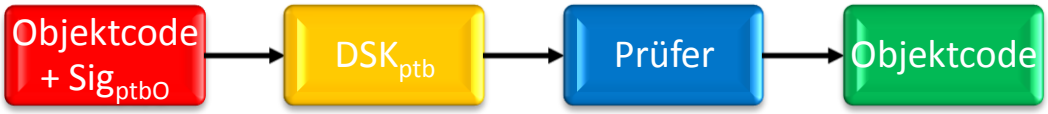



Bild 34a: Abgesicherte Übernahme des Objektcodes durch den Prüfer

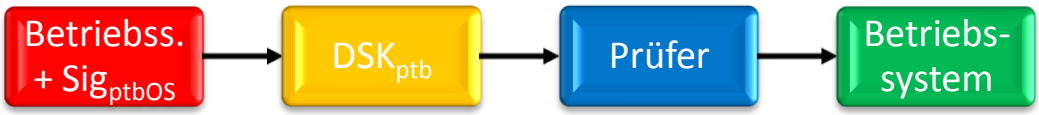



Bild 34b: Abgesicherte Übernahme des Betriebssystems durch den Prüfer

Liegen Objektcode und Betriebssystem vor, müssen diese zusammen mit einer eindeutigen Hardwarekennung, (welche das Gerät eindeutig identifiziert) so in Zusammenhang gebracht werden, dass eine Gerätesignatur $Sig_{svG}$ erzeugt werden kann, mit der sich diese einmalige Kombination aus Hard- und Software authentifizieren lässt und womit sie ihre Ausgaben signieren kann.

Der hier aufgeführte Begriff *GUID* (Globally Unique Identifier) bezieht sich auf das Ergebnis eines Algorithmus, der verschiedene Parameter der Gerätehardware abfragt und zu einer Kennzeichenfolge kombiniert.

Ein übliches „Infektionsszenario“ würde das Einspielen von Betriebssystem und Software, das Hochfahren des Geräts und das anschließende Einspielen von Wächter und Schutzmantel vorsehen. Hier läge jedoch ein unnötiges Risiko vor. Denn es müsste sichergestellt werden, dass am Gerät auch tatsächlich Betriebssystem und Software ausschließlich mit Wächter und Schutzmantel eingespielt werden. Dabei entstehen zwei Risiken: Zum einen, dass der Sachverständige zuerst eine vollständige Installation vornimmt und dokumentiert und diese anschließend erneut ohne Schutzmaßnahmen vornimmt. Zum anderen, dass Dritte dies nachträglich durchführen. In beiden Fällen ist kein eindeutiger Nachweis darüber möglich, wer es gemacht hat.

Praktischer und eindeutiger wäre das Ausliefern von Betriebssystem und Software in bereits „modifizierter“ Form durch die Zulassungsstelle, mit entsprechender Signatur. Der Übergang der Software vom Sachverständigen zum Gerät wäre somit kein Risiko mehr.

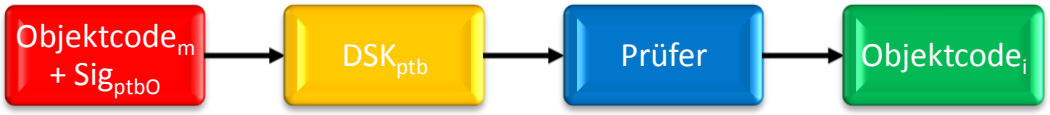



Bild 35a: Abgesicherte Übernahme des modifizierten Objektcodes durch den Prüfer

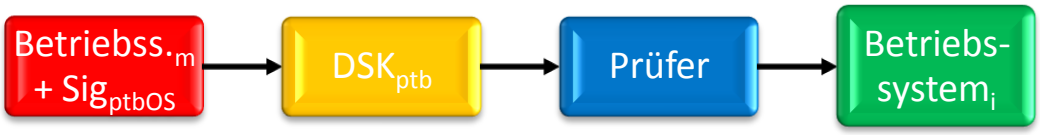



Bild 35b: Abgesicherte Übernahme des modifizierten Betriebssystems durch den Prüfer

Werden Betriebssystem und Anwendung gestartet, wird zunächst das Wächterprogramm instanziiert und erzeugt als erste Handlung die fünf Werte $GUID_{HW}$, $Größe_O$, $Größe_{Oi}$, $Hash_O$ und $Hash_{Oi}$. Dabei werden die Größe des modifizierten Objektcodes in Byte und ein daraus generierter Hash-Wert jeweils für den eingespielten und den anschließend infizierten Objektcode ermittelt.

Im folgenden Diagramm wird aufgezeigt, wie die Verifikationspfade ausgebildet sind. Durch die von einem Trust Center erzeugten öffentlichen Signaturschlüssel für Hersteller, PTB und Sachverständige werden sämtliche verwendeten Signaturen verifizierbar. Alle vom Wächter erzeugten Werte sind ebenfalls indirekt oder direkt damit verifizierbar.

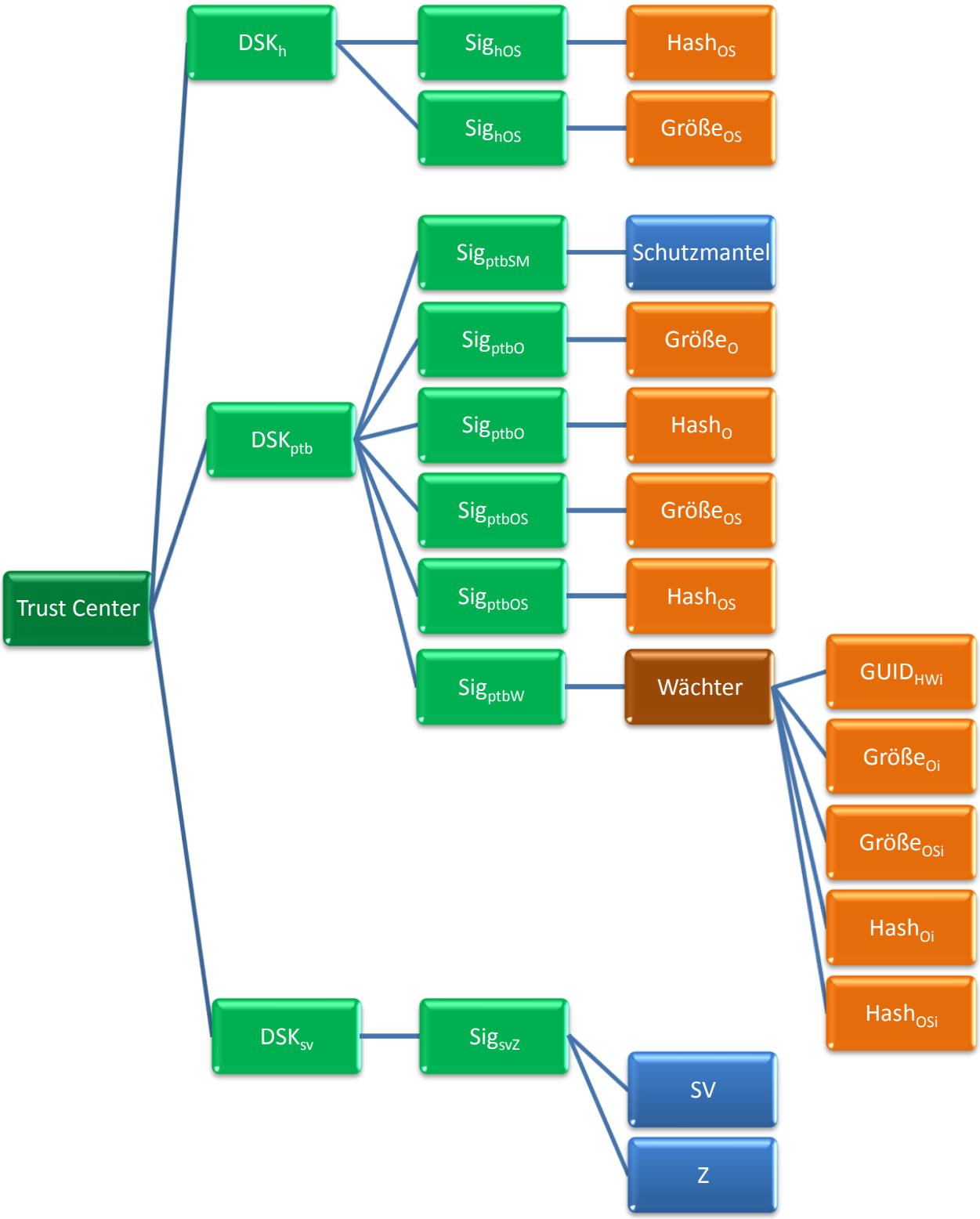



Bild 36: Verifikationsbaum

Die folgende Tabelle zeigt auf, welche Einzeldaten in das Gerät eingespielt werden, welche in den Dongle überspielt werden müssen, wie diese von ihrer Entstehungsreihenfolge im Zusammenhang zueinander stehen und wodurch sie verifiziert werden können.

| Hersteller | => | PTB | => | SV | => | Gerät | Dongle | Verifikation |
|---|---|---|---|---|---|---|---|---|
| $Sig_{hOS}$ | $DSK_h$ | Betriebssystem | | | | | | |
| | | ↓ | | | | | | |
| | | Schutzmantel | | | | | | |
| | | Wächter | | | | | | |
| | | ↓ | | | | | | |
| | | $Betriebssystem_m$ | | | | | | |
| | | $Sig_{ptbOS}$ | $DSK_{ptb}$ | $Betriebssystem_m$ | => | $Betriebssystem_i$ | | $Sig_{ptbOS}$ |
| $Sig_{hS}$ | $DSK_h$ | Sourcecode | | | | | | |
| | | ↓ | | | | | | |
| | | Objektcode | | | | | | |
| | | Schutzmantel | | | | | | |
| | | Wächter | | | | | | |
| | | ↓ | | | | | | |
| | | $Objektcode_m$ | | | | | | |
| | | $Sig_{ptbO}$ | $DSK_{ptb}$ | $Objektcode_m$ | => | $Objektcode_i$ | | $Sig_{ptbO}$ |

| | | |
|---|---|---|
| Wächter | $GUID_{HWi}$ | Wächter |
| | $Größe_O$ | $Sig_{ptbO}$ |
| | $Größe_{OS}$ | $Sig_{ptbOS}$ |
| | $Größe_{Oi}$ | Wächter |
| | $Größe_{OSi}$ | Wächter |
| | $Hash_O$ | $Sig_{ptbO}$ |
| | $Hash_{OS}$ | $Sig_{ptbOS}$ |
| | $Hash_{Oi}$ | Wächter |
| | $Hash_{OSi}$ | Wächter |
| | SV | $Sig_{svZ}$ |
| | Z | $Sig_{svZ}$ |
| | $Sig_{svZ}$ | $DSK_{sv}$ |
| | $Sig_{hOS}$ | $DSK_h$ |
| | $Sig_{ptbOS}$ | $DSK_{ptb}$ |
| | $Sig_{ptbO}$ | $DSK_{ptb}$ |
| | $Sig_{ptbSM}$ | $DSK_{ptb}$ |
| | $Sig_{ptbW}$ | $DSK_{ptb}$ |
| | $DSK_{sv}$ | Trust Center |
| | $DSK_{ptb}$ | Trust Center |
| | $DSK_h$ | Trust Center |
| | $ECK_{sv}$ | I/O-Komm. |
| | $ECK_{ptb}$ | I/O-Komm. |
| | $ECK_h$ | I/O-Komm. |

Tabelle 4: Gesicherte Übergänge

Die Wächter-Software erzeugt Daten bzw. verfügt über Daten, die unmittelbar nach Installation der Software vom Sachverständigen in den Dongle übertragen werden müssen. Die Übertragung der Geräteparameter aus dem Gerät an einen PC des Sachverständigen kann über dieselbe Schnittstelle geschehen, wie das Einspielen der Software. Am PC ließe sich dann der Dongle programmieren. Die übertragenen Geräteparameter sind nach dem Anstecken des Dongle am Gerät für Schutzmantel und Wächterprogramm zugänglich. Dadurch nehmen beide ihre Arbeit auf und vergleichen diese Angaben ab da regelmäßig mit den selbst ermittelten Werten.

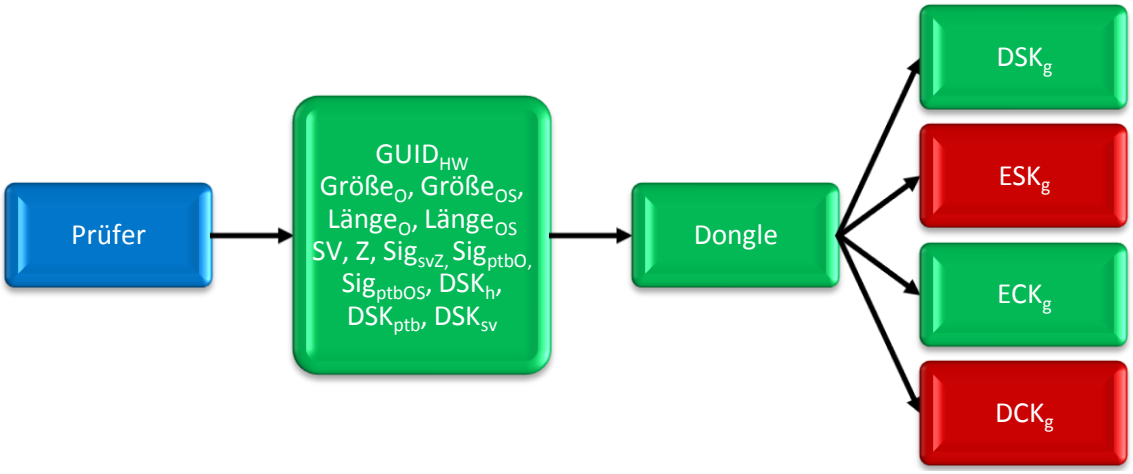



Bild 37: Initialisierung des Geheimnisträgers durch den Prüfer

## 14 Kryptografisch abgesicherte Prüfung nach § 7 SpielV

Diese Prüfung ist im Soll-Prozesses unsinnig, muss aber aufgrund der Gesetzeslage möglicherweise berücksichtigt werden. Zumindest werden Zeitaufwand und Risiko eines Geräteschadens gegenüber dem Ist-Prozess erheblich vermindert.

Im ersten Schritt erfolgt ein einfaches Challenge-/Response-Verfahren, wobei auch hier darauf zu achten ist, dass der öffentliche Enkodierschlüssel aus einer öffentlichen Quelle und nicht vom Gerät stammt. Damit wird verhindert, dass eine falsche Software scheinbar korrekte Ergebnisse liefert. Dabei ist *m* ein Zeitstempel, der mit einer zufälligen Verzögerung angezeigt wird, damit er nicht hochaktuell ist und vom Gerät erraten werden kann.

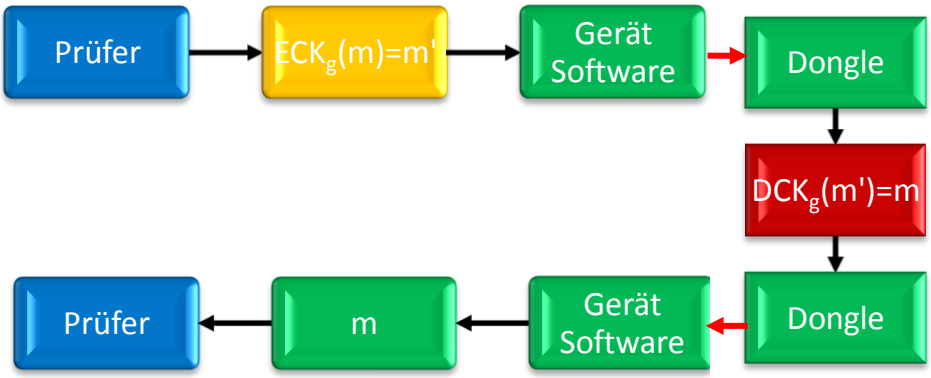



Bild 38: Challenge/Response zur Authentifizierung des Geräts

Zusätzlich sendet das Gerät eine Signatur mit einem zweiten signierten Zeitstempel *Z* als zusätzlicher und zu dokumentierender Nachweis, dass der Prüfer korrekt geprüft hat.

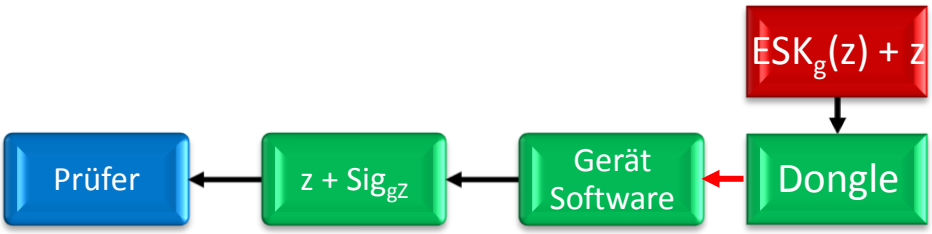



Bild 39: Nachweis der korrekten Prüfung

Nach Erhalt von *Z* und dessen Signatur $Sig_{gZ}$ kann diese jederzeit mit dem öffentlichen Signaturschlüssel $DSK_g$ verifiziert werden, wobei dieser nicht vom Gerät geliefert werden sollte.

Entsprechend 12.1 erfolgt die gezeigte Kommunikation selbst noch einmal innerhalb eines abgesicherten Protokolls.

Es bietet sich für diesen gesamten Vorgang eine einfache Softwarelösung an, um die für einen Nachweis relevanten Daten *m, m', z* und $Sig_{gZ}$ zu dokumentieren. Diese könnte auch gleichzeitig sicherstellen, dass nur die nach der Freischaltung hinterlegten öffentlichen Schlüssel zum Einsatz kommen.

Obwohl der Prüfer bei der Überprüfung auf eine falsche Signatur stoßen kann, wäre diese jederzeit auch ohne Prüfer und Überprüfung durch eine Kontrolle der signierten Geräteausgaben festzustellen.

## 15 Absicherung

Das erklärte Ziel eines vollständig erfolgreichen Angriffs auf das aufgezeigte Konzept muss darin bestehen, sämtliche eingehenden Kommunikation weiterhin zu entschlüsseln und zu interpretieren und nach außen gehende Kommunikation weiterhin korrekt zu signieren, trotz vollständiger Kontrolle des Angreifers über das Gerät und seine Software.

Ein Angriff, der anschließend keine korrekte kryptografische Funktionalität mehr erlaubt, kann jederzeit durch entsprechende Kontrolle der Ausgabedaten des Geräts oder durch Kommunikationsprobleme entdeckt werden und ist somit nur begrenzt nützlich, da eindeutig nachweisbar.

Sollte es gelingen, brachliegende und unentdeckte unerwünschte Funktionalität im laufenden Code auszulösen, so hängt es davon ab, ob die Ziele eines Angreifers ohne Kommunikation mit der Außenwelt sinnvoll und vollständig umsetzbar sind oder diese eine Kommunikation erfordern. Letzteres ließe sich anhand einer verschlüsselten Protokollierung nachweisen.

Das Gerät gilt als vollständig kompromittiert, wenn die vollständige Kontrolle über das Gerät durch den Angreifer gegeben ist und weiterhin korrekt signiert und entschlüsselt werden kann.

Das Gerät gilt als kompromittiert, wenn die vollständige Kontrolle über das Gerät durch den Angreifer gegeben ist, aber kein korrektes Signieren und Entschlüsseln mehr möglich ist.

Das Gerät gilt als teilweise kompromittiert, wenn keine Kontrolle über das Gerät durch den Angreifer gegeben ist, dadurch weiterhin korrekt signiert und entschlüsselt werden kann, aber das Gerät unerwünschte Funktionalität ausführen kann, die jedoch protokolliert wird.

Nach dieser Definition sind alle Geräte die dem Ist-Prozess unterliegen als vollständig kompromittiert einzustufen. Natürlich fehlen die kryptografischen Sicherheitsmaßnahmen. Aber auch ein Gerät, dessen Binärcode sich durch beliebiges Austauschen jeglicher Kontrolle entziehen lässt, ist für einen entsprechenden Angreifer vollständig kontrollierbar.

Gelänge es einem Angreifer, eine unerwünschte Funktionalität in den Code einzubringen und diese ohne weitere Kommunikation vollständig und erfolgreich im Sinne des Angriffs ausführen zu lassen, wäre das Gerät ebenfalls vollständig kompromittiert.

Das Gerät wird dann außer Betrieb gesetzt, wenn bereits eine teilweise Kompromittierung oder ein Betrieb ohne Dongle festgestellt wird.

- zum einen durch gezieltes Überschreiben von Anwendungs- und Betriebssystemcode,
- zum anderen durch ein Zerstören des Dongles.

Wird ein Gerät ohne Dongle betrieben, verliert die Software ihre eigentliche Funktionalität, bleibt aber noch in der Lage, den wieder angebrachten Dongle zu erkennen und ebenfalls zu zerstören.

Das „Zerstören“ kann in der Praxis z. B. durch das Herabsetzen eines „Unit Counter für Pay-per-Use“ [wibu1] oder ein ähnliches Konzept realisiert werden, welches letztendlich dem Auslaufen einer Lizenz gleichkommt.

## 15.1 Angriffspunkte

Mit Kenntnis aller privaten und öffentlichen Schlüssel sowie der entsprechenden kryptografischen Algorithmen wäre das Gerät jederzeit und vollständig kompromittierbar. Um an die Schlüssel zu gelangen, muss man entweder an den Inhalt des Dongle kommen, die ursprüngliche Schlüsselerzeugung exakt nachvollziehen können oder mit Kryptoanalyse die privaten Schlüssel ermitteln. Alternativ kommen „Man in the Middle"-Attacken oder Ähnliches in Frage, die entweder den unverschlüsselten Datenstrom abfangen, manipulieren und weiterleiten oder sich zwischen die Kommunikationspartner stellen, damit diese nur noch indirekt und unbemerkt über den Angreifer kommunizieren können. Wenn es einem Angreifer gelänge, die Installation in seinem Sinne vollständig zu manipulieren, könnte dieser eigene Signaturen erzeugen.

Offensichtlicher Angriffspunkt ist der Dongle. Die Herausforderung besteht darin, durch Umstecken des Dongles auf einen PC (bei ausgeschaltetem Spielgerät) die im Dongle verwahrten privaten Schlüssel auszulesen, um für eine eigene Anwendungssoftware korrekte Signaturen erzeugen und Dechiffrierungen vornehmen zu können.

Ein zweiter Angriffspunkt liegt darin, den Dongle vollständig zu umgehen und eigene Schlüssel zu verwenden.

Ein weiterer Angriffspunkt auf die Sicherheit liegt in der unkontrollierten Kommunikation über die Hardwareschnittstellen. Weist die Anwendung bereits im Sourcecode Hintertüren auf, die nicht erkannt werden oder weist das Betriebssystem einen Objektcode auf, der beispielsweise gezielt Daten oder Parameter für die laufende Anwendung manipuliert, um damit deren Verhaltensweise zu verändern, so wäre das mit Signaturen nicht zu verhindern, da sich der Objektcode im laufenden Betrieb nicht ändert.

### 15.1.1 Angriffe während der Installation

Die folgende Tabelle zeigt auf, welche Auswirkungen bestimmte Angriffe haben, die vor oder während der Installation erfolgen können. Idealerweise sind diese direkt erkennbar, wobei sich das Gerät außer Betrieb setzt (AB). Ansonsten sind immer die Signaturen fehlerhaft oder nicht vorhanden, was jedoch überprüft werden kann.

| Angriff / Abwehr | Schutzmantel | Wächter | Obj.code | $Sig_{ptbO}$ | $Sig_{ptbOS}$ | $Sig_{g}$ |
|---|---|---|---|---|---|---|
| Falscher Objektcode | Komm | AB | | Ja | | |
| Falsches Betriebssystem | Komm | AB | | | Ja | |
| Tausch des Objektcodes | Komm | AB | | Ja | | Indirekt |
| Tausch des Betriebssystems | Komm | AB | | | Ja | Indirekt |
| Weglassen des Dongles | AB | AB | AB | | | |

Tabelle 5: Auswirkungen möglicher Angriffe

Da der Sachverständige grundsätzlich nur bereits „vorinfizierte" Software erhält, die zudem noch entsprechend signiert ist, kann dieser nur die Installation als Ganzes umgehen, nicht jedoch die ausgelieferte Software ohne Überwachungssoftware installieren.

**Fazit:** Das Konzept ist dahingehend ausreichend sicher, dass aktive Angriffe durch den Prüfer immer nachweisbar sind und andere Angriffe dazu führen, dass das Gerät außer Betrieb gesetzt wird.

### 15.1.2 Angriffe während des Betriebs

| Angriff / Abwehr | Schutzmantel | Wächter | Obj.code |
|---|---|---|---|
| Entfernung Dongle | AB | AB | AB |
| Tausch Dongle | Komm | AB | AB |
| Tausch Schutzmantels | Komm | AB | AB |
| Entfernung Schutzmantels | Komm | AB | AB |
| Tausch Betriebssystem | Komm | AB | AB |
| Tausch Anwendung | Komm | AB | AB |
| Zusatzanwendung | Komm | AB | |
| Aktivierung Schadcode (I/O) | Komm | | |
| Aktivierung Schadcode (Timer) | Komm | AB | |
| Entfernung Wächter | Komm | AB | AB |
| Tausch Hardware | AB | AB | AB |
| Komm von Außen | Komm | | |
| Komm von Innen | Komm | | |
| Analyse Betriebssystem | Komm | | |
| Analyse Objektcode | Komm | | |
| Analyse Wächter | Komm | | |
| Analyse Schutzmantel | Komm | | |

Tabelle 6: Auswirkungen möglicher Angriffe während des Betriebs

Im laufenden Betrieb verhindert der Schutzmantel mit seiner Überwachung der Hardwareschnittstellen eine ungewünschte Kommunikation mit der Außenwelt, sodass Eingriffe in das Gerät nur über die erlaubten Kommunikationskanäle und deren Protokolle möglich sind. Diese Eingriffe werden vom Schutzmantel jedoch unterbunden. Lediglich ein bewusst im Objektcode oder Betriebssystem hinterlegter Schadcode könnte während des Betriebs zur Ausführung kommen, sofern dieser bei einem Code-Review übersehen wurde. Um eine Kompromittierung der Gerätesicherheit herbeizuführen, müsste dieser Code jedoch am Schutzmantel vorbei mit der Außenwelt kommunizieren oder seine Kommunikation im Rahmen der Protokolle abwickeln, welche eine eindeutige Zuordnung des Kommunikationspartners zulassen. Nur wenn ein Schadcode ohne jegliche Kommunikation arbeiten kann und keine Modifikationen am laufenden Code vornimmt, wird dieser nicht entdeckt. Denkbar wäre in diesem Zusammenhang eine andere statistische Verteilung des Spielverlaufs im normalen Betrieb gegenüber dem Messbetrieb durch die PTB.

**Fazit:** Das Konzept ist dahingehend ausreichend sicher, dass lediglich ein Schadcode im Betriebssystem oder im Objektcode nicht direkt erkannt werden kann, jedoch dessen Kommunikation nach Außen kontrolliert wird.

### 15.1.3 Angriffe nach Ausschalten des Geräts

Nach erfolgter zugelassener Inbetriebnahme des Geräts muss dieses vollständig ausgeschaltet werden, um weitere Angriffe vornehmen zu können. Die Sicherheit wird in diesem Falle durch das Wächterprogramm gewahrt, welches sich im System festsetzt. Nur bei vollständiger Entfernung des Wächterprogramms und nicht gestarteter Software (Betriebssystem oder Anwendung) kann ein Angreifer das Zerstören des Dongle verhindern.

**Fazit:** Das Konzept ist dahingehend ausreichend sicher, dass es in der Praxis einen hohen individuellen Aufwand für jedes Gerät verlangt, um dessen Dongle auszulesen und die neue Anwendungssoftware darauf abzustimmen und einzuspielen.

## 16 Vergleich zwischen Ist- und Soll-Prozess

Ein **Umgehen der Sicherheit** ist nur noch durch ein vollständiges Ersetzen der Gerätesoftware möglich und jederzeit über Stichproben anhand fehlender bzw. gefälschter Signaturen erkennbar. D.h., ein Umgehen der Sicherheit wäre mit großem Aufwand zunächst noch denkbar, aber letztlich immer eindeutig nachweisbar. Damit wäre eine solche Manipulation im flächendeckenden Stil aufgrund des Entdeckungsrisikos nicht mehr praktisch umsetzbar, sodass dieses Sicherheitsrisiko grundsätzlich auf gering herabgestuft werden könnte.

Die **Bevorzugung eines Herstellers** durch Mitarbeiter der PTB wäre ebenfalls deutlich schwieriger zu bewerkstelligen. Zwar würde es dazu weiterhin genügen, zu Beginn der Bauartmusterprüfung vom Hersteller eingebrachte Sicherheitsrisiken in Gerätehard- und –software bewusst zu ignorieren, durch die notwendige Einbindung eines Wächterprogramms können die Auswirkungen jedoch überprüfbar gemacht werden. Auch hier erlaubt das neue Verfahren, im Nachhinein Manipulationen dieser Art eindeutig forensisch nachzuweisen.

**Unbeabsichtigte Fehler** bleiben vom Soll-Prozess unberührt und müssen von einem angemessen anspruchsvollen Verfahren zur Qualitätssicherung erkannt werden.

Das Risiko der **persönlichen Bereicherung**, insbesondere durch Mitarbeiter des Herstellers, würde deutlich reduziert, da die zusätzlichen Sicherheitsmechanismen eine Manipulation erheblich erschweren und – wenn diese gelänge – nachweisbar machen würden.

Dasselbe trifft für **Manipulationen durch Aufsteller** zu.

**Manipulationen durch Sachverständige** dürfen ebenfalls als gering eingestuft werden, da durch den Soll-Prozess, der nur noch eine Freischaltung und keine Prüfung mehr vorsieht, die Anzahl der Prüfer reduziert wird und einzelne Manipulationen einen hohen Aufwand verlangen.

**Manipulationen durch zugelassene Stellen** müssen jedoch immer noch als mittelmäßig eingestuft werden, da eine flächendeckende, herstellerbezogene Freischaltung noch genügend finanziellen Spielraum lässt, um den hohen Aufwand zu rechtfertigen, den das Vorbereiten und Installieren manipulierter Software erfordern würde. Allerdings besteht auch hier die Nachweisbarkeit, wobei diese hinsichtlich einer Konstellation aus „zugelassenen Stellen + Hersteller + Mitarbeiter PTB“ durch nachträgliches Wiederfreischalten eines Geräts prinzipiell umgangen werden könnte.

Das folgende Bild vergleicht die Risikoeinschätzung des Ist-Prozesses mit der des geplanten Soll-Prozesses. Das reduzierte Risiko verlagert sich auf die unmittelbare Einflusssphäre der PTB.

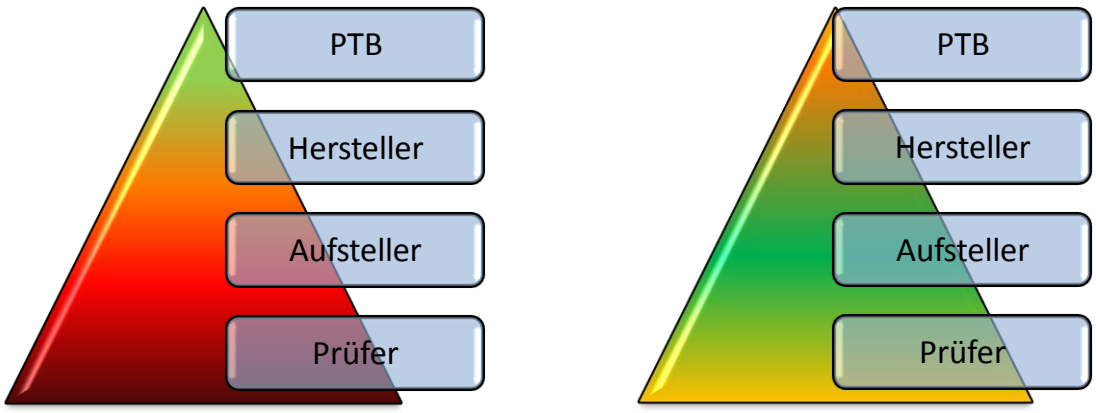



Bild 40: Risikopyramide des Ist-Prozesses und Risikopyramide des Soll-Prozesses

## 16.1 Soll-Ist-Vergleich der Risikoanalyse

Im Folgenden der Vergleich der Risikoanalysen für Ist- und Soll-Prozess.

| | Gerät | PTB | Hersteller | Aufsteller | SV | Zugelassene Stellen | MA PTB | MA Hersteller | MA Aufsteller |
|---|---|---|---|---|---|---|---|---|---|
| **Umgehung der Sicherheit** | | | | | | | | | |
| **Bevorzugung eines Herstellers** | | | | | | | | | |
| **Unbeabsichtigte Fehler** | | | | | | | | | |
| **persönliche Bereicherung** | | | | | | | | | |
| **Manipulationen durch Aufsteller** | | | | | | | | | |
| **Manipulationen durch Sachverständige** | | | | | | | | | |
| **Manipulationen durch zugelassene Stellen** | | | | | | | | | |
| ***Maximales Schadensrisiko*** | | | | | | | | | |

| Legende | | | |
|---|---|---|---|
| **Sehr hoch** | **Hoch** | **Mittel** | **Gering** |

Tabelle 7: Sicherheitsrisiken des Ist-Prozesses

| | Gerät | PTB | Hersteller | Aufsteller | SV | Zugelassene Stellen | MA PTB | MA Hersteller | MA Aufsteller |
|---|---|---|---|---|---|---|---|---|---|
| **Umgehung der Sicherheit** | | | | | | | | | |
| **Bevorzugung eines Herstellers** | | | | | | | | | |
| **Unbeabsichtigte Fehler** | | | | | | | | | |
| **persönliche Bereicherung** | | | | | | | | | |
| **Manipulationen durch Aufsteller** | | | | | | | | | |
| **Manipulationen durch Sachverständige** | | | | | | | | | |
| **Manipulationen durch zugelassene Stellen** | | | | | | | | | |
| ***Maximales Schadensrisiko*** | | | | | | | | | |

| Legende | | | |
|---|---|---|---|
| **Sehr hoch** | **Hoch** | **Mittel** | **Gering** |

Tabelle 8: Sicherheitsrisiken des Soll-Prozesses

## 16.2 Optimierung der Sicherheit

Das Restrisiko der nicht mehr notwendigen zweijährigen Prüfung ist am Fuße der Soll-Pyramide (Bild 40) noch zu erkennen. Das Verlagern der Prüfung auf die Freischaltung reduziert die Anzahl notwendiger Prüfungen erheblich, erhöht aber im Zuge dessen die Anforderungen an diejenigen Prüfer deutlich, welche ein Gerät für die Inbetriebnahme freischalten.

Wird einem Gerät 6 bis 8 Jahre Laufzeit unterstellt, wären heute im zweiten, vierten und sechsten Jahr – also bis zu drei - Prüfungen notwendig. Der Soll-Prozess würde somit die Anzahl Prüfungen halbieren bzw. dritteln. Daraus folgt, wie bereits in 8.6 ausgeführt, dass durch die Verlagerung des Prüfzeitpunktes die eigentliche Prüfung und die damit verbundene Prüfungsaufgabe entfallen.

Die Verringerung der benötigten Prüfungen aufgrund des Soll-Prozesses eröffnet grundsätzlich die aus Überlegungen der Sicherheit, Wirtschaftlichkeit und fachlichen Anforderungen sinnvolle Möglichkeit, ausschließlich öffentlich bestellte und vereidigte Sachverständige für das Sachgebiet 2100 (ggf. mit einer Zusatzqualifikation für Geldspielgeräte) mit der Freischaltung zu betrauen.

Damit wären die Risikofaktoren „Sachverständiger für Sachgebiet 530“ und „zugelassene Stellen“ vollständig ausgeschaltet.

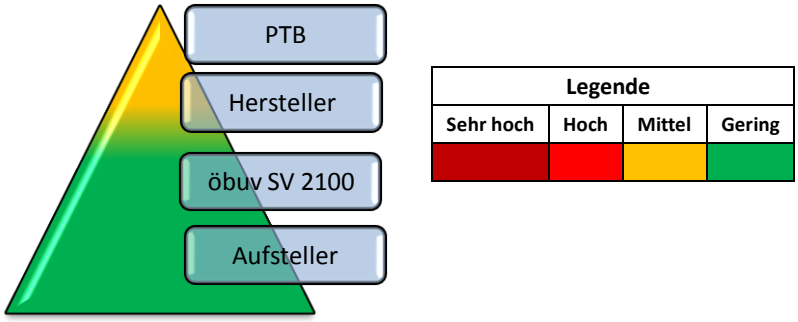



Bild 41: Risikopyramide des optimierten Soll-Prozesses

| | Gerät | PTB | Hersteller | Aufsteller | SV 2100 | MA PTB | MA Hersteller | MA Aufsteller |
|---|---|---|---|---|---|---|---|---|
| **Umgehung der Sicherheit** | | | | | | | | |
| **Bevorzugung eines Herstellers** | | | | | | | | |
| **Unbeabsichtigte Fehler** | | | | | | | | |
| **Persönliche Bereicherung** | | | | | | | | |
| **Manipulationen durch Aufsteller** | | | | | | | | |
| **Manipulationen durch Sachverständige** | | | | | | | | |
| **Manipulationen durch zugelassene Stellen** | | | | | | | | |
| ***Maximales Schadensrisiko*** | | | | | | | | |

Tabelle 9: Sicherheitsrisiken des optimierten Soll-Prozesses

Eine interessante Erkenntnis bezüglich der einzelnen Risikoeinstufungen besteht darin, dass diese im Wesentlichen die Tatsache reflektieren müssen, dass sie vorhanden sind und vereinfacht werden sollen. Ob dabei Begriffe wie „sehr hoch“, „mittel“ etc. zur Anwendung kommen oder eine andere Form der Differenzierung verwendet wird, ist nicht so relevant wie die Zielsetzung, möglichst alle wichtigen Risiken identifizieren und anschließend wirksam reduzieren zu können. Nur wenn dies nicht in allen Fällen gelingt oder die Fülle an Einzelrisiken nicht bewältigt werden kann, kommt der Qualität einer Risikoeinstufung eine besondere Bedeutung zu.

Mit anderen Worten: Auch wenn in 6.4 eine andere Einstufung der Risiken denkbar gewesen wäre, hätte dies nichts daran geändert, dass die Risiken nahezu alle ausgeschaltet werden konnten. Ist ein solches Ergebnis absehbar, können unter Umständen langwierige Begriffsfindungen entfallen.

## 16.3 Weitere denkbare Vereinfachungen

Eine zweite, in dieser Arbeit nicht näher besprochene Möglichkeit, wäre der Einsatz einer Virtuellen Maschine, innerhalb derer die Software des Geräts ablaufen müsste. Eine solche VM könnte Anforderungen an die in ihr ablaufenden Anwendungen stellen, die eine normale Gerätehardware nicht erfüllen kann, aber welche die VM simuliert. Zwar müsste für jede Gerätearchitektur eine eigene VM entwickelt werden, dafür wäre jedoch die Gerätesoftware einheitlich programmierbar und vor der Zulassung einfacher überprüfbar – z. B. durch Unit-Tests oder andere automatisierte Prüfverfahren für Software.

Die Virtuelle Maschine könnte die Aufgaben des Schutzmantels bei der Absicherung der Kommunikation und der Kommunikationskanäle übernehmen und beispielsweise das Ablaufen nur einer Anwendung erzwingen.

Trotzdem wäre die Virtuelle Maschine immer noch entsprechend nach außen hin zu sichern, damit nicht parallel weitere Software ausgeführt werden kann, welche die Sicherheit beeinträchtigen könnte.

## 17 Theorie trifft Praxis

Grundsätzlich stellen sich nach erfolgter Analyse des Ist-Konzepts und des Entwurfs eines möglichen Soll-Konzepts folgende Fragen:

- Warum wurde nicht sofort ein sicheres Konzept umgesetzt?
- Hat dies Auswirkungen für eine nachträgliche Umsetzung auf ein sicheres Soll-Konzept?

Aus der zeitlichen Nähe der Risikoanalyse eines bis dahin nur theoretisch bekannten Ist-Konzepts zu der praktischen Prüfung der ersten Geldspielgeräte durch den Autor im April und Mai 2008 ergab sich die Gelegenheit zur Beurteilung der tatsächlichen Umsetzung durch die PTB.

Bei der praktischen Geräteprüfung hatte der Autor bei seinen ersten vier Geräteprüfungen bereits zwei Stück (2002 JAZZ – adp und 2003 NEON – Bally-Wulff), die mindestens 20 Cent des Spielers verspielen, bevor dieser die Abbuchungsautomatik ausschalten kann. Dieses Verhalten steht im direkten Widerspruch zu § 13 SpielV *„Es ist eine Bedienvorrichtung für den Spieler vorhanden, mit der er vorab einstellen kann, ob aufgebuchte Beträge unbeeinflusst zum Einsatz gelangen oder jeder einzelne Einsatz durch Betätigung geleistet wird.“*. Daraus war zu folgern, dass entweder die PTB die Geräte fälschlicherweise zum Vorteil des Herstellers und Nachteil des Spielers entgegen dem Gesetzestext zugelassen hat oder dass die Software trotz identischer CRC32-Checksumme ein anderes Verhalten als zum Zeitpunkt der Zulassungsprüfung aufgezeigt hat.

Fehler bei der Zulassung wurden von der PTB am 06.05.2008 letztlich als Ursache für diese Diskrepanz genannt [ptb6] und die Bestätigung der Zulassung des Geräts gefordert.

Einige Tage später wurde ein Gerät „2005 NEW WINNER“ von adp geprüft, welches sofort € 2,-- aufgrund eines „Sonderspiels“ verspielte. Auch hier wurde von der PTB am 07.05.2008 ein Fehler bei der Zulassung als Ursache genannt [ptb6].

Bis zum 16.06.2008 wurde dieser Sachverhalt an keinen der sonstigen am Ist-Prozess Beteiligten Prüfer, Hersteller oder Aufsteller kommuniziert. Erst in einem Newsletter vom 16.06.2008 [ptb7] wurde dieser Sachverhalt von der PTB vage erwähnt und die Bescheinigung der Konformität verlangt.

Durch diese Vorgehensweise einzelner Mitarbeiter der PTB wird von den Prüfern verlangt, die Ungleichbehandlung von Geräten und Herstellern zu bestätigen und aufrecht zu erhalten. Die Motivation der PTB hierfür kann von Bequemlichkeit über Inkompetenz bis zur Bestechung oder Erpressung einzelner Mitarbeiter durch einen bevorzugten Hersteller reichen, was die Bedeutung des Risikos PTB/Hersteller unterstreicht (siehe 7.2 und 7.8).

Der Autor sieht keinerlei technische oder fachliche Gründe, die der ursprünglichen Umsetzung eines brauchbaren Konzepts im Wege hätten stehen können. Die folgenden Negativbeispiele dienen nochmals zur Verdeutlichung:

- Promovierte Mathematiker und Statistiker der PTB müssen mit der korrekten Vorgehensweise zur Ermittlung von aussagekräftigen Messwerten vertraut sein (8.1).
- Wer immer bei der PTB die über 100 Zulassungen auf monatlicher Basis als PDF-Dateien pflegt (www.ptp.de/spielgeraete, Menüpunkt „Zulassungen“) und aktualisiert, sollte erkennen, dass hiermit eine fehlerträchtige organisatorische Hürde für den einzelnen Sachverständigen und den Ist-Prozess im Allgemeinen entsteht.

- Die PTB bietet den Sachverständigen keine Möglichkeit, die Überprüfung des Binärcodes über die serielle Schnittstelle eines Geldspielgeräts ohne die – teils kostenpflichtige – Software des Herstellers vorzunehmen.
- Die PTB bestätigte schriftlich, dass Gerätezulassungen erteilt wurden, die gegen § 13 SpielV verstoßen, aber diesen Geräten trotzdem die Bestätigung der erfolgreichen Prüfung durch den Sachverständigen zu erteilen ist – trotz der Möglichkeit Softwareupdates als Nachträge zur Zulassung zwingend vorzuschreiben und trotz eindeutiger gesetzlicher Vorschriften.

Definitiv bestätigen bereits die ersten belegbaren Praxisbeispiele einen Gesamteindruck von Intransparenz und Subjektivität und weisen deutlich auf ein fehlendes Qualitätsmanagement hin.

Im Falle der Zulassungsdokumente gab es mehrfach detaillierte und schriftliche Vorschläge von Sachverständigen, dass eine ZIP-Datei über alle Zulassungsdokumente und eine ZIP-Datei über alle aktuellen Änderungen die sinnvollere und mit Minimalaufwand implementierbare praktische Lösung wäre. Trotzdem wird seitens der PTB weiterhin von einem hohen Aufwand für eine nicht erkennbare Datenbankproblematik gesprochen und keine Lösung implementiert. Das Risiko, einem Gerät aufgrund einer veralteten Zulassung eine Prüfplakette für weitere zwei Jahre zu geben, steigt damit für den Sachverständigen erheblich.

Die Risikoanalyse wurde am 5.3.2008 abgeschlossen. Die obigen Informationen und Erkenntnisse wurden dem Autor erst nach diesem Datum bekannt. Diese Eindrücke bestätigen somit im Nachhinein die Ergebnisse der Risikoanalyse, dass auch die PTB einen sehr hohen Risikofaktor darstellt.

### 17.1 Maßnahmen

Die im Folgenden genannten Einzelschritte zur Umsetzung der theoretischen Erkenntnisse in die Praxis sind unter den oben genannten Umständen vermutlich zum Scheitern verurteilt. Bereits einfachste Sicherheitsmaßnahmen wie die Implementierung von ZIP-Dateien oder die Dokumentation von Schnittstellenprotokollen sind zum Stand 22.06.2008 von der PTB nicht umgesetzt worden. Die Umsetzung komplexerer Maßnahmen durch eine Partei, die selbst ein erhebliches Sicherheitsrisiko darstellt und bereits Unsicherheiten in den Prozess eingebracht hat, erscheint dem Autor deshalb sehr unwahrscheinlich.

Erschwerend kommt hinzu, dass für eine umfassende Umstellung auf einen sicheren Soll-Prozess bereits im Ansatz Änderungen an zukünftiger Gerätehardware nötig sind und sich diese nicht kurzfristig implementieren lassen werden.

Deshalb werden die folgenden Einzelmaßnahmen in Sofortmaßnahmen, mittel- und langfristige Maßnahmen unterteilt und deren jeweiligen Gesamtauswirkungen betrachtet.

### 17.1.1 Sofortmaßnahmen

Die wirkungsvollste Sofortmaßnahme besteht in der Einführung einer „qualifizierten elektronischen Signatur“ für die Hersteller. Da diese den rechtlichen Stellenwert einer Unterschrift besitzt und die Geldspielgeräte alle über herstellerseitige Sicherheitsmaßnahmen verfügen, um einen unzulässigen Betrieb zu verhindern, wäre die vertragliche Verpflichtung, die „qualifizierte elektronische Signatur“ diesen Sicherheitsmaßnahmen zugrunde zu legen, einfach und naheliegend. Käme es nämlich zum Einsatz von Software in Geldspielgeräten, die nicht von der PTB zugelassen wurde, ergäben sich zwei Möglichkeiten:

- Entweder ist diese falsche Software korrekt signiert - woraus sich eindeutig Verantwortung und Haftung des Herstellers ergeben
- oder die Software ist falsch signiert, womit dem Hersteller umgehbare Sicherheitsmaßnahmen nachgewiesen wären, für deren Vorhandensein er ebenfalls eindeutig die Verantwortung trägt.

Die „qualifizierte elektronische Signatur“ muss auch für die PTB eingeführt werden.

- Mit dieser sind immer komplette Archive von Zulassungen zu signieren.
- Die Zulassungen sind mit einem einheitlichen Verfallsdatum zu versehen.
- Das Archiv benötigt eine Änderungshistorie.

Daraus ergeben sich Maßnahmen zur Risikominimierung für die Sachverständigen, die jedoch eine klare Nennung der jetzigen Verantwortungsübergänge verlangen:

- Es muss klar und eindeutig kommuniziert werden, dass die aktuelle Form der Binärcodeprüfung keine Aussage über dessen Relevanz für den Betrieb des gerade untersuchten GeldspielGeräts besitzt, da für den Sachverständigen nicht überprüfbar.
- Das Auslesen und die Überprüfung des Binärcodes haben grundsätzlich mit Software zu erfolgen, die der Sachverständige bestimmt und beibringt. Dazu müssen die Schnittstellenprotokolle für Sachverständige offengelegt werden.
- Der ausgelesene Binärcode muss anhand einer „qualifizierten elektronischen Signatur“ des Herstellers verifiziert werden, um dessen rechtliche Verantwortung dokumentieren zu können und um eine sichere Alternative zum CRC32-Algorithmus zu verwenden.
- Die Zulassungsprotokolle müssen anhand eines mit „qualifizierter elektronischer Signatur“ signierten Archivs vorliegen, über ein monatliches Verfalldatum verfügen und mit Änderungshistorie versehen sein, um eine eindeutige Verantwortung der PTB bezüglich der Inhalte der Zulassungen zu gewährleisten.

Hiermit ließen sich sofort folgende Einzelrisiken ausschließen:

- Die fälschliche Interpretation der Prüfungsergebnisse als aussagekräftig und damit eine Verantwortung des Sachverständigen hierfür gegenüber Dritten.
- Die erzwungene Abhängigkeit des Sachverständigen zu den Herstellern und der PTB und damit fehlende Neutralität, Objektivität und Unabhängigkeit.
- Die Haftung des Sachverständigen bei fehlerhaften/veralteten Zulassungen durch die PTB.
- Das Risiko für PTB und Sachverständige bei nichtzugelassener Software des Herstellers.

Folgende Einzelrisiken ließen sich zumindest reduzieren:

- Die Verwendung veralteter Zulassungen durch den Sachverständigen.
- Der Einsatz gefälschter Software ohne Kenntnis des Herstellers.

### 17.1.2 Mittelfristige Maßnahmen

Vor Ort gewonnene Erkenntnisse bezüglich fehlerhafter Zulassungen, Sicherheitsrisiken im Ist-Prozess, Optimierungen des Prozessablaufs etc. verlangen nach einem Qualitätsmanagement durch die PTB, um Fehler der Vergangenheit durch Nachträge aus der Welt zu schaffen und momentan nicht abstellbare Sicherheitsrisiken zumindest überwachen zu können.

Diese Maßnahmen sind deshalb als mittelfristig zu bezeichnen, da sie eine weitergehende Analyse des Zulassungsprozesses verlangen, um weitere, bisher unerwähnte oder unentdeckte Sicherheitsrisiken auffinden zu können. Beispielsweise müsste zusätzlicher Zeitaufwand darauf verwendet werden, die Verfahren zur Ermittlung des statistischen Verhaltens der Geräte zu untersuchen bzw. festzustellen ob deren Messergebnisse ebenso anzuzweifeln sind, wie die der implementierten Prüfkonfigurationen.

Insofern verlangen die jetzigen Auswirkungen des Ist-Prozesses schon deshalb nach einem Qualitätsmanagement, um eine nachträgliche Gleichbehandlung aller Hersteller bzw. deren Geräte herbeizuführen.

- Die Umsetzung verlangt die Beantragung von jeweils einer „qualifizierten elektronischen Signatur“ durch jeden Hersteller und durch die PTB.
- Die Hersteller müssten zu jeder Softwareversion eine Signatur mit ihren geheimen Schlüsseln erzeugen.
- Die Hersteller müssten ihre Software dahingehend anpassen, dass der Binärcode mit seiner Signatur eingespielt wird und der Binärcode selbst sich anhand der Signatur und einem extern zugänglichen öffentlichen Schlüssel (z. B. in vorhandener Chipkarte) regelmäßig verifiziert.
- Der Hersteller muss seinen öffentlichen Schlüssel veröffentlichen.
- Die PTB muss ihre Zulassungen zukünftig als Archiv mit Historie und Signatur zugänglich machen.
- Die PTB muss ihren öffentlichen Schlüssel veröffentlichen.

Diese Maßnahmen sollten sich bei entsprechender Planung innerhalb eines Monats nach Erhalt der „qualifizierten elektronischen Signatur“ durch jede der betroffenen Parteien umsetzen lassen.

### 17.1.3 Langfristige Maßnahmen

Die Sofortmaßnahmen können im Wesentlichen lediglich dazu beitragen, Transparenz über eindeutig nachvollziehbare Verantwortungsbereiche herbeizuführen und die Problembereiche im Ist-Prozess zu isolieren. Die mittelfristigen Maßnahmen befassen sich hauptsächlich mit Maßnahmen zur Sicherung der Qualität, der Analyse noch unbekannter Problembereiche und der nachträglichen Absicherung bekannter Probleme.

Langfristige Maßnahmen befassen sich mit der Beseitigung der herstellerseitigen Risiken. Dabei wären Änderungen an bestehenden Hardwarearchitekturen ebenso nötig wie die Entwicklung neuer und die Anpassung vorhandener Software.

Wie in 8.1 gezeigt, ist das implementierte Prüfkonzept über die Messschnittstelle nicht sicher, da dem Gerät mittels Protokoll mitgeteilt wird, dass und wie es geprüft werden soll. Eine Lösung als „Transparent Bridge“ würde diese Prüfkonfigurationen weiterhin nur der PTB zugänglich machen. Durch die Verschlüsselung des Datenverkehrs wäre nicht nur die bestehende von der PTB geforderte einfache Passwortabfrage überflüssig, sondern grundsätzlich die Sicherheit dieser Schnittstelle auf ein vernünftiges Maß erhöht.

In der Praxis würde ein PC bei ausgeschaltetem Geldspielgerät als „Man in the Middle“ eingeschleift werden und mit einer Software analog zu Wireshark ausgestattet sein, um den Netzwerkverkehr zu protokollieren. Nur wenn der kryptografische Schlüssel bekannt ist, ließe sich der mitgehörte Datenverkehr auch dekodieren und manipulieren.

Indem der PC entweder die eine oder andere Schnittstelle des Geräts bedient, ist auch die Simulation von Spielsteuerung und Kontrolleinrichtung möglich.

Hiermit lassen sich weitere Sicherheitsmaßnahmen implementieren:

- Die Brücke muss Kontrolleinrichtung und Spielsteuerung, wie in der „Technischen Richtlinie“ gefordert, trennen. D.h. umgekehrt, ein Gerät dürfte auf keinen Fall arbeiten, wenn diese Brücke aufgetrennt wurde. Wenn doch, wäre dies bei Entdeckung belegbar.
- Werden Zusatzgeräte an anderen Schnittstellen betrieben, lässt sich anhand der Brücke prüfen, ob deren Kommunikation mit dem Geldspielgerät auch tatsächlich im verlangten Maße über die Kontrolleinrichtung erfolgt.

### 17.2 Grenzen der Umsetzung

Spätestens bei den langfristigen Maßnahmen wird klar, dass diese auf den Widerstand der Hersteller stoßen werden. Damit werden auch die Grenzen aufgezeigt, denen das Umsetzen eines sicheren Prozesses unterliegt: Je mehr Parteien mitreden können, desto länger wird die Umsetzung dauern und desto weniger wird letztlich von dem umgesetzt, was umgesetzt werden sollte. Insofern ist nach Meinung des Autors das Umstellen auf einen sicheren Prozess nur mit klaren Maßgaben möglich, die in diesem Falle vom Gesetzgeber vorzugeben sind bzw. konsequent einzufordern wären.

Allerdings zeigt die Risikoanalyse auch, dass sich der jetzige Prozess schon dadurch sicherer machen ließe, wenn nur eine Partei, in diesem Falle die PTB, ihren Aufgaben- und Verantwortungsbereich konsequent am Sicherheitsgedanken ausrichten würde.

Ein funktionierender konsequenter Zulassungs- und Prüfungsprozess würde dazu führen, dass Geräte nicht oder nicht mehr zugelassen werden, die jetzt noch mit fehlerhaften Zulassungen, die aufgrund mangelnden Qualitätsmanagements erteilt wurden, in Betrieb sind. Dasselbe Qualitätsmanagement würde sowohl deutlich mehr Probleme vor der Zulassung aufdecken wie auch schneller die Nachbesserung nach erteilter Zulassung einfordern.

Dies würde zu dem in der Industrie beobachteten Effekt führen, dass nur noch ein unbedingtes Einhalten von Qualität und Sicherheit durch die Hersteller eine wirtschaftliche Alternative gegenüber der jetzigen Vorgehensweise darstellt.

Dieser Gedanke ließe sich auch auf die Überprüfung übertragen. Anstatt von vielen Prüfern sinnlose Prüfungen durchführen zu lassen, wären Sourcecode-Reviews mit den wenigen dafür qualifizierten Sachverständigen dem Qualitätsgedanken sehr viel zuträglicher. Solange keine langfristigen Maßnahmen bezüglich der Geräte- und Softwarearchitektur umgesetzt sind, wären Fehler, Hintertüren, fehlende Struktur oder sonstige Ungereimtheiten im Sourcecode einer Zulassung hinderlich. Hier würde auch wieder das Prinzip greifen, dass es auf Dauer als Hersteller wirtschaftlicher ist, einen gut prüfbaren Sourcecode ohne Beanstandungsmöglichkeiten abzuliefern, als keine Zulassung zu erhalten.

## 17.3 Alternative Umsetzung

Mit Stand 09.05.2008 erhielt der Autor Kenntnis über eine Veröffentlichung einer Stellungnahme des Wissenschaftsrates zur PTB vom 08.05.2008 [wr1]. Auf Seite 14 wird Folgendes festgestellt:

*1. Aufgabenentwicklung: Um die Kohärenz des Tätigkeitsspektrums auch in Zukunft zu erhalten, sollte die PTB nicht mit Aufgaben betraut werden, die dem wissenschaftlichen Profil der Einrichtung widersprechen. Routinetätigkeiten wie die Prüfung von Schusswaffen, Geldspielgeräten und elektronischen Wahlgeräten sollten anderweitig organisiert werden.*

Das Ergebnis dieser Masterarbeit zeigt auf, dass die PTB sich nicht in der Lage zeigt, eine der genannten Routinetätigkeiten umzusetzen. Es liegt nahe, dass dies für die anderen genannten Routinearbeiten ebenso zutrifft. Die Risikoanalyse würde deshalb auch die Alternative zulassen, den Risikofaktor PTB gänzlich aus dem Prozess herauszunehmen und deren Aufgaben durch eine entsprechend qualifizierte Organisation durchführen zu lassen.

## 18 Zusammenfassung

Eine Betrachtung der technischen Umsetzung der Spielverordnung SpielV unter den Aspekten „Sicherheit“ und „Stand der Technik“ kann nur zu dem Schluss kommen, dass weder „Sicherheit“ noch „Stand der Technik“ gegeben sind.

Sowohl der Vergleich zwischen Ist- und Soll-Prozess wie auch die Vorgehensweise zur praktischen Umsetzung eines sicheren Soll-Prozesses zeigen die einfache technische Machbarkeit eines aussagekräftigen und sicheren Konzepts nach dem Stand der Technik auf.

Gerade die technische Machbarkeit eines sicheren Konzepts hätte für Fachleute bereits in der Entwurfsphase so offensichtlich sein müssen, wie umgekehrt die Unzulänglichkeiten des tatsächlich entworfenen Konzepts. Ebenso offensichtlich muss es für Fachleute gewesen sein, dass das jetzige Konzept hohe Hürden für eine nachträgliche Absicherung und Abänderung bereithält.

Auch ohne die Aspekte „Sicherheit“ und „Stand der Technik“ besonders betonen zu müssen, ist aus technischer Sicht das Verfahren zur Bauartzulassung der Physikalisch-Technische Bundesanstalt unsicher und ohne Aussagekraft. Wichtige in § 13 SpielV genannte Anforderungen werden nicht erfüllt, ohne dass es hierfür überzeugende fachliche Gründe gibt.

Das Überprüfungsverfahren für Geldspielgeräte nach § 7 SpielV, wie es von der PTB vorgestellt wurde, erfüllt ebenfalls nicht die elementarsten fachlichen Kriterien für einen sicheren und nachweisbaren Überprüfungsprozess, wie sie von öffentlich bestellten und vereidigten Sachverständigen normalerweise vorausgesetzt werden. Auffallend ist hierbei, dass die Kritikpunkte direkt auf die Einflussnahme der PTB auf den Überprüfungsprozess zurückzuführen sind.

Dies führt unmittelbar zu einer Ungleichbehandlung von Geräten und Herstellern.

Die Schlussfolgerung daraus ist, dass die in § 8 (11) der Sachverständigenordnung gestellten Anforderungen nicht zu erfüllen sind, womit Rolle und Aufgabe der öffentlich bestellten und vereidigten Sachverständigen unklar sind.

Da dieselbe Fachabteilung der PTB auch für die in die öffentliche Kritik geratene Zulassung von Wahlcomputern verantwortlich zeigt, stellt sich die berechtigte Frage, ob die in dieser Arbeit aufgeführten Sicherheitsrisiken nicht auch auf die Zulassung von Wahlcomputern zutreffen könnten.

**Quellenverzeichnis**


[adp1] Prospekt „Erneute Prüfung nach § 7 SpielV“, adp Merkur Service und TÜV Rheinland

[adp2] Betriebsanleitung Geld-Gewinn-Spiel-Geräte, Ausgabe NSV 1, S. 37, adp Gauselmann GmbH

[adp3] Handbuch Filialmonitor 4.1, S. 3, adp Gauselmann GmbH

[adp4] http://www.openpr.de/news/137014/50-Jahre-Gauselmann-Gruppe-Innovations-und-Technologiefuehrer-der-Automatenbranche-feiert-stolzes-Jubilaeum.html

[adp5] Sachverständigenschulung adp Gauselmann am 30.01.2008 in Lübbecke

[awi1] Broschüre „Faktum 06“ des AWI Automaten-Wirtschaftsverbände-Info GmbH

[bes1] http://www.blickpunkt-euskirchen.de/rag-ewi/docs/100122/lokales

[ct1] c’t magazin für computer technik – Ausgabe 24/2006, Seite 72

[dbt1] Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Harald Terpe, Birgitt Bender, Elisabeth Scharfenberg, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN – Drucksache 16/5516 – Gewährleistung des Spielerschutzes bei Geldspielgeräten

[dom1] http://85.25.136.73/domann-p28h15s16--ADP-Datenbank-o.html

[isa1] http://www.isa-guide.de/articles/14826_uavd_fordert_weiterreichende_nderungen_oder_eine_erneute_novellierung_der_spielverordnung.html

[ptb1] Inhalt der Geräteüberprüfungen

[ptb2] „Technische Richtlinie – Zur Sicherung der Prüfbarkeit und Durchführung der Bauartprüfung von Geldspielgeräten im Sinne von § 33c Gewerbeordnung“, Version 4.0

[ptb4] Bauart-Zulassung für Geldspielgeräte Nr.: 2001 Name: „GRAFFITY“, Seite 4, als Muster für weitere Bauartzulassungen

[ptb5] Vertrag PTB – zugelassene Stellen

[ptb6] E-Mail-Korrespondenz des Autors mit der PTB vom 07.05.2008

[ptb7] Informationen und Hinweise für Inspektoren vom 16. Juni 2008

[spielv1] IV. Zulassung von Spielgeräten – Bekanntmachung der Neufassung der Spielverordnung vom 27. Januar 2006

[spielv2] § 7 – Bekanntmachung der Neufassung der Spielverordnung vom 27. Januar 2006

[sv1] http://www.krueger-automaten.de/html/unternehmen/firmengruppe.php, Verweis der Firmengruppe Bauriedel auf die Unternehmensberatung Stephan Bauriedel.

[sv2] http://www.spielautomaten-pruefung.de/, Sachverständigenseite des Stephan Bauriedel

[sv3] http://www.sachverstaendiger-geldspielgeraete.de/index.php?option=com_content&task=view&id=7&Itemid=28, Sachverständigenseite des Herrn Daloglu.

[sv4] Gutachten des Herrn Daloglu als Angestellter der PTB, Seite 25, zum Zwecke der öffentlichen Bestellung durch die IHK.

[svo1] http://www.ihk-schwaben.de/dokumente/merkblaetter/M44967.pdf

[uadv1] Prüfbericht der PTB zu dem in [dbt1] genannten Verfahren gegen adp Gauselmann http://www.uavd.de/images/stories/ptb_prfbericht.pdf

[wibu1] WIBU-Systems, CodeMeter Entwickler-Handbuch, Seite 33, Januar 2008

[wr1] Stellungnahme zur Physikalisch-Technischen Bundesanstalt (PTB), Braunschweig und Berlin, Mai 2008 (Drs. 8477-08)

[www1] http://www.forum-glueckspielsucht.de/news/show.php?id=2724