DOI 10.2195/lj_NotRev_stockenberger_de_201111_01

Integrierte Sicherheitsmerkmale als Schutz vor Produktpiraterie im Maschinen- und Anlagenbau

Integrated Security Features to Protecting against Counterfeiting in Mechanical Engineering

DIPL.-WI.-ING. DOMINIK STOCKENBERGER
DIPL.-ING. JANINA DURCHHOLZ
PROF. DR.-ING. DIPL.-WI.-ING. WILLIBALD A. GÜNTHNER
fml – LEHRSTUHL FÜR FÖRDERTECHNIK MATERIALFLUSS LOGISTIK

Zusammenfassung

Die Bedrohung durch Produktpiraterie wächst ständig, besonders der deutsche Maschinen- und Anlagenbau ist mehr und mehr davon betroffen. Um Komponenten und Ersatzteile zu schützen, wurde ein technisches Konzept zur Abwehr von Produktpiraterie entwickelt. In diesem System werden Teile mit kopiersicheren Echtheitsmerkmalen gekennzeichnet, welche an diversen Identifikations- und Prüfpunkten entlang der Supply-Chain und besonders beim Einsatz in der Maschine ausgelesen und geprüft werden. Die Prüfergebnisse werden in einer zentralen Datenbank gespeichert, um neue Services zu ermöglichen und die Kommunikation zwischen Hersteller und Kunde zu erleichtern.

Abstract

The menace of counterfeiting is growing constantly, especially the German mechanical engineering is more and more attractive to copyists. To protect components and spare parts, there is a technical concept for anti-counterfeiting developed. In this system, the parts are tagged with fraud proof marks which are read out at several checking points along the supply chain and particularly within the machine. The checking results are stored in a central database in order to create new services and to simplify the communication between manufacturer and customer.

1. Produktpiraterie und Schutztechnologien

Produktpiraterie- und Kopierschutztechnologien sind vielfältig aus dem Alltag und prominenten Beispielen bekannt. Diese werden unter anderem auf Verpackungen eingesetzt, welche von Konsumenten als erstes wahrgenommen werden und die Kaufentscheidung beeinflussen (vgl. Abbildung 1).
Im Bereich des Maschinen- und Anlagenbaus sind ganzheitliche Konzepte für einen umfassenden Schutz vor Produktpiraterie nicht verbreitet und systematisiert eingeführt: „Das Verfolgen durchgängiger Schutzstrategien, die die gesamte Wertschöpfungskette von den Lieferanten bis zum Kunden einbeziehen, stellt einen akuten Handlungsbedarf der Industrie dar“ [Wildemann et al. 07]. Dabei ist das Erkennen der Pirateriewaren eine Grundlage der wirksamen Bekämpfung von Produktpiraterie. Die Kopien von Bau- und Ersatzteilen erreichen oftmals ein so hohes Qualitätsniveau, dass die Identifikation der Pirateriewaren schwierig ist [Wildemann et al. 07] (vgl. Abbildung 2). Um den Schutz von Originalbauteilen und -produkten zu gewährleisten, gibt es verschiedene Möglichkeiten [Wildemann et al. 07]:

- Produktkennzeichnung und -authentifizierung
- Verfolgung und Überwachung der Produkte
- gegenseitige Authentifizierung von Produkten und Komponenten.

Dabei bildet bei Produkten ohne eigene Intelligenz ein zusätzlich aufgebrachtes oder integriertes Kennzeichen die Grundlage für Verfolgung und Überwachung sowie Authentifizierung.

Personalausweis:

holografisches Portrait, 3-D-Bundesadler, kinematische Bewegungsstrukturen, Makro-, Mikroschrift, Kontrastumkehr, holografische Wiedergabe der maschinenlesbaren Zeilen, maschinell prüfbare Struktur, Oberflächenprägung, mehrfarbige Guillochen, Laserbeschriftung, Wasserzeichen ([Bundesministerium des Inneren 05a], [Bundesministerium des Inneren 05b])

Fahrkarten, Eintrittskarten und Tickets:

Sicherheitsmerkmale wie spezielle Einfärbungen, Hologramme, Wasserzeichen, UV-fluoreszierende Fasern etc. ([Halbach 11], [Mitsubishi HiTec Paper 11], [Pipimaru 11]

Handy-Akkus der Nokia GmbH:

Hologramm ([Chip Online 04], [Nokia Corporation 11])

Baustoffe der Knauf Gips KG:

Sicherheitsmarkierung mit Hologramm, thermoreaktive Farbe ([Schreiner Group 11], [Völcker 06])

Verpackungen:

Klebeetiketten mit Secutag® Mikrofarbcodes ([3S Simons 11], [von Welser 07])

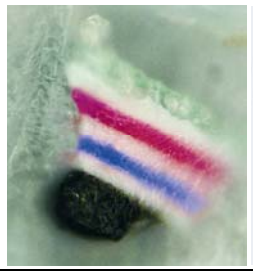


Abbildung 1: Verschiedene Sicherheitstechnologien in diversen Produkten und prominenten Beispielen

Abbildung 2: Original und Kopie (Quelle: APM - Aktionskreis gegen Produkt- und Markenpiraterie e.V.)

Zum Schutz von Ersatzteilen und Komponenten des Maschinen- und Anlagenbaus wurde im Forschungsprojekt ProAuthent[1] ein integrierter Produktpiraterieschutz durch Kennzeichnung und Authentifizierung entwickelt. Dabei wurde am Lehrstuhl fml ein methodisches Vorgehen gewählt, welches als validiertes Vorgehen für Unternehmen empfohlen wird, die ihre Produkte durch Kennzeichnung und Authentifizierung vor Produktpiraterie schützen wollen:

1. Auswahl von schützenswerten Bauteilen
2. Auswahl passender Kennzeichnungstechnologien
3. Integration der Kennzeichen in die schützenswerten Bauteile
4. Errichtung eines Identifikations- und Prüfpunktes (IP-Punkt)
5. Integration der IP-Punkte in ein IT-Gesamtsystem
6. Realisierung von Zusatznutzen

Diese Schritte werden in den nächsten Abschnitten detailliert beschrieben.

2. Auswahl schützenswerter Bauteile

In Unternehmen des Maschinen- und Anlagenbaus sind vor allem lukrative Komponenten und Ersatzteile betroffen ([Günthner et al. 08], [Wildemann et al. 07], [VDMA 10]). Daher ist es im ersten Schritt zur Kennzeichnung und Authentifizierung von Bau- und Ersatzteilen wichtig zu untersuchen, welche Bauteile wirklich schützenswert sind. Denn ein Schutz aller Bauteile eines Unternehmens mit Hilfe von Kennzeichnungstechnologien ist nicht wirtschaftlich, der Schutz aller von Produktpiraterie betroffenen Bauteile teils zu aufwändig, teils nicht ausreichend. Im Forschungsprojekt ProAuthent haben sich die in Abbildung 3 gelisteten Kriterien zur Auswahl der schützenswerten Bauteile bewährt. Dabei entsprechen die schützenswerten Bauteile immer den Basiskriterien. Weitere Bauteile können identifiziert werden, wenn die optionalen Kriterien zusätzlich herangezogen werden.

[1] ProAuthent - Integrierter Produktpiraterieschutz durch Kennzeichnung und Authentifizierung von kritischen Bauteilen im Maschinen- und Anlagenbau. Das Forschungs- und Entwicklungsprojekt wurde mit Mitteln des Bundesministeriums für Bildung und Forschung (BMBF) innerhalb des Rahmenkonzeptes „Forschung für die Produktion von morgen“ gefördert und vom Projektträger Forschungszentrum Karlsruhe (PTKA) betreut (Laufzeit: 01.01.2007 – 31.03.2011).

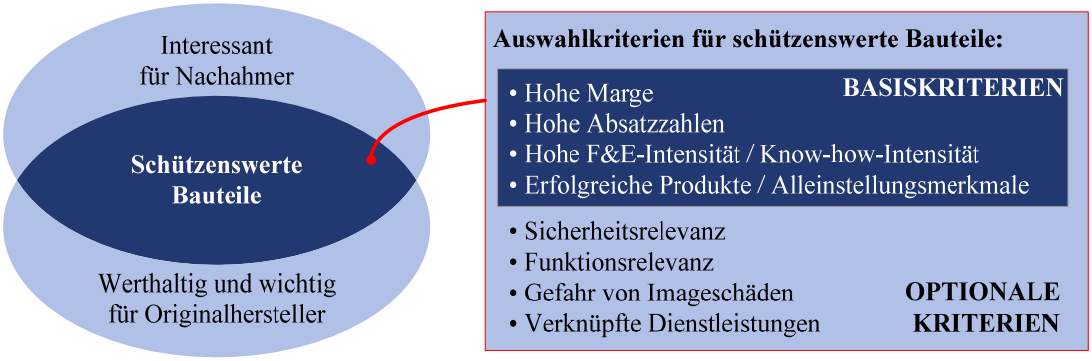


Abbildung 3: Kriterien zur Auswahl der schützenswerten Bauteile (Quelle: Lehrstuhl fml)

3. Auswahl passender Kennzeichnungstechnologien

Nach Bestimmung der schützenswerten Bauteile muss eine Auswahl der je Bauteil passenden Kennzeichnungstechnologie erfolgen. Vor der Nutzung eines kopiersicheren Echtheitsmerkmals, um die Produkte als Original oder Unikat zu markieren, sollten diese Bauteile aber immer mit einem auf dem entsprechenden Markt geschützten Markenlogo des Unternehmens gekennzeichnet sein. Dieses Markenlogo sollte möglichst an nicht nachträglich einzubauenden Teilen integriert, nicht nachträglich aufbringbar und möglichst von außen sichtbar sein (z.B. Einbringen des Logos in einer Gussform, vgl. Abbildung 4). [Wildemann 08]

Abbildung 4: Bauteil mit Firmenlogo: Kettenplatte der HOMAG (Quelle: HOMAG Holzbearbeitungssysteme GmbH)

Um eine sichere Unterscheidbarkeit zwischen Original und Kopie jederzeit garantieren zu können und Bauteile bei Bedarf zusätzlich maschinell auf Originalität prüfen zu können, sind über das Markenlogo hinaus entsprechende Kenzeichnungstechnologien auszuwählen und zu nutzen. Zur Bestimmung einer Kennzeichnungstechnologie und somit eines kopiersicheren Merkmals für ein schützenswertes Bauteil werden zunächst die Anforderungen aus der Herstellung und Verwendung des Teils sowie der Nutzung des späteren Kennzeichens aufgenommen. Diese lassen sich in technische sowie betriebswirtschaftliche Einflussgrößen gliedern.

Technische Einflussgrößen [Abele et al. 10]:

- Die im Merkmal gespeicherte Information
- Die erreichbare Zugänglichkeit bei der Prüfung
- Der akzeptable Prüfaufwand
- Der erforderliche Automatisierungsgrad
- Die verfügbare Infrastruktur für die Prüfung

Betriebswirtschaftliche Einflussgrößen (in Anlehnung an [Abele et al. 10]):

- Gesamte Investitionsbereitschaft in Kennzeichnungstechnologien
- Kosten für Kennzeichnungstechnologien sowie deren Implementierung am Produkt bzw. deren Prüfinfrastruktur
- Qualitative Größen (möglicher Zusatznutzen, gerichtliche Verwertbarkeit, Imageverlust durch Nachahmungsfälle, Phase des Produktlebenszyklus)

Diese Einflussgrößen wurden im Forschungsprojekt genau definiert und deren Ausprägungen für die 31 gelisteten Kennzeichnungstechnologien (vgl. Tabelle 1) erarbeitet. Wichtig ist der folgende Mechanismus: Über die Ausprägungen der Einflussgrößen je schützenswertem Bauteil sowie den Ausprägungen der Einflussgrößen je Kennzeichnungstechnologie lässt sich die größtmögliche Übereinstimmung zwischen Anforderungen des Bauteils und Möglichkeiten der Kennzeichnungstechnologie und somit die passende Kennzeichnungstechnologie je Bauteil bestimmen.

1D-Barcode	Laseroberflächenauthentifizierung
2D-Barcode	Magnetcode
Akusto-/elektromagnetisches Merkmal	Magnetfarbe
Clusterfolie	Markennamen, -zeichen
Codes mit Rauschmustern	Markierung im Sinterbauteil
Coin-Reactive-Ink	Musteroberfläche/Oberflächenmuster
Data Trace	Pen-Reactive
Digitaldruck / PrePress-Druckmerkmale	RFID (Radiofrequenzidentifikation)
DNA-Markierung	Röntgenfluoreszenz
Echtfarbenelement / Leuchtfarben	Sicherheitsanstanzung
Farbcode (Microcode, Microtaggant, Secutag)	Sicherheitsstreifen, Sicherheitsfaden
Fotochrome Farbe	Siebdruck, Prägen
Hologramm/Optically Variable Device (OVD)	Stochastische Schwankungen im Fertigungsprozess
Intagliodruck	Thermoreaktive, thermochrome, thermische Farbe
IR-/UV-Farbpigmente	Wasserzeichen
Kippfarbe	

Tabelle 1: Kennzeichnungstechnologien zur Erzeugung von Sicherheitsmerkmalen (Quelle: Lehrstuhl fml)

Das Ergebnis dieser Auswahl für die beteiligten Anwenderunternehmen ist in Abbildung 5 zu sehen. Es wurden die vier, in Abbildung 6 näher beschriebenen Kennzeichnungs- und Authentifizierungstechnologien als die im Maschinen- und Anlagenbau besten Technologien bestimmt. Dabei handelt es sich bei IR-Farben sowie Hologrammen um Originalitätskennzeichen, bei RFID und CDP um Unikatkennzeichen. Originalitätskennzeichen sind Kennzeichen mit fälschungssicheren Merkmalen, bei Unikatkennzeichen sind diese Merkmale zusätzlich einmalig [Wildemann et al. 07].

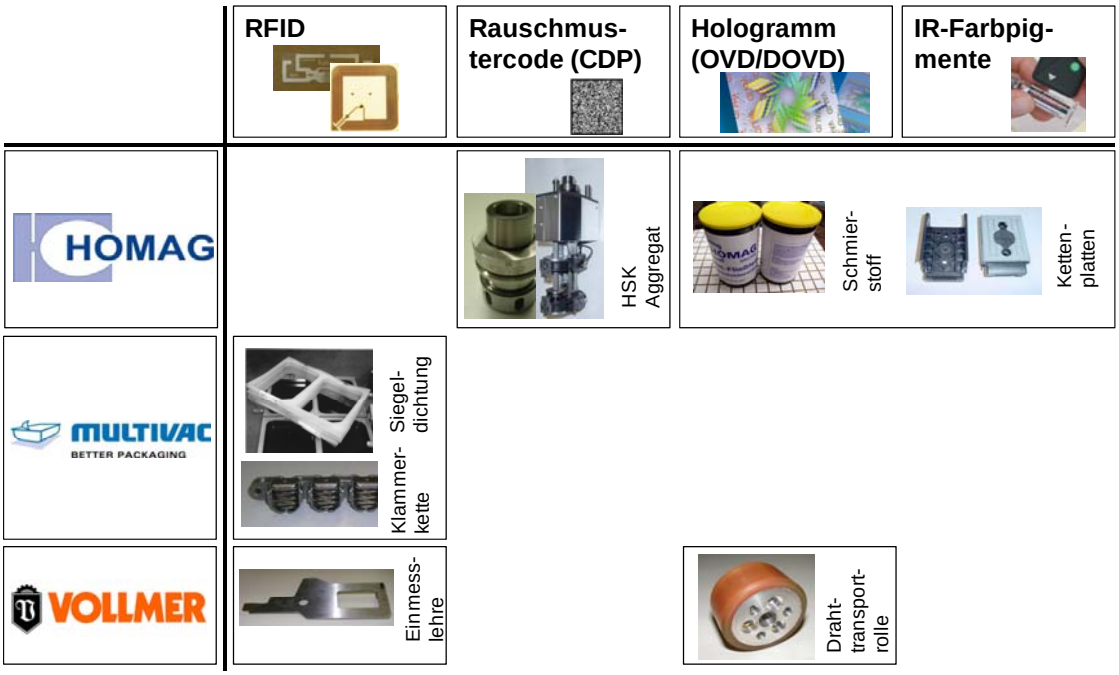


Abbildung 5: Kennzeichnungstechnologie je schützenswertem Bauteil der Anwenderunternehmen (Quelle: HOMAG Holzbearbeitungssysteme GmbH, Multivac Sepp Haggenmüller GmbH & Co. KG, Schreiner Group GmbH & Co. KG, VOLLMER WERKE Maschinenfabrik GmbH, Lehrstuhl fml)

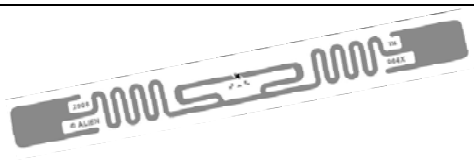
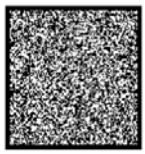
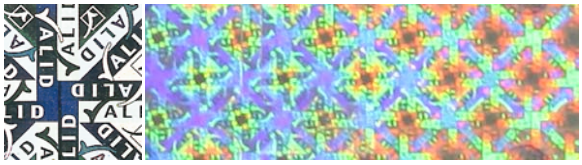
RFID (Radiofrequenz-Identifikation): Auto-ID-Technologie, deren Transponder (Mikrochip mit Antenne zur (elektro-) magnetischen Kopplung) mit Schreib-Lesegeräten berührungslos erfassbar, auslesbar und beschreibbar sind.	 **UHF-Transponder ALN-964X Squiggle® Inlay [Alien Technology 11]**
CDP (Copy Detection Pattern): Gedrucktes Rauschmuster das mit optischen Lesegeräten authentifizierbar, aber nicht kopierbar ist.	 **CDP (Quelle: Schreiner Group GmbH & Co. KG)**
IR-Farben (Infrarot-Farben): Farbpigmente, die mit Lesegeräten detektierbar und aufgrund der im Einzelfall spezifischen Farbmischung kopiersicher sind.	 **IR-Klebeetikett – die IR-Farbpigmente sind für das menschliche Auge unsichtbar (Quelle: Schreiner Group GmbH & Co. KG)**
Hologramm: Aufwendig erzeugte Abbildungen, die bei Beleuchtung mit gleichartigem Licht ein dreidimensionales Abbild eines Gegenstands erscheinen lassen und nicht kopierbar sind.	 **Hologramm als Druckvorlage (li.) sowie als Klebeetikett (Quelle: Schreiner Group GmbH & Co. KG)**

Abbildung 6: Kennzeichnungstechnologie je schützenswertem Bauteil der Anwenderunternehmen

4. Integration der Kennzeichen in schützenswerte Bauteile

Ziel der Integration der Sicherheitsmerkmale in die schützenswerten Bauteile ist es, den folgenden für alle Installationen dieser Art grundlegenden Anforderungen zu genügen (in Anlehnung an [ICC 06], [Winkler, Wang 07]):

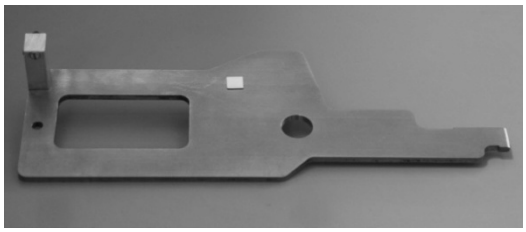
1. Eindeutigkeit:
   Das Sicherheitsmerkmal muss das Objekt eindeutig als Original erkennbar machen, d.h. ein Sicherheitsmerkmal darf weltweit nicht zufällig mehrfach existieren.
2. Fälschungssicherheit:
   Das Sicherheitsmerkmal darf nur mit größtmöglichem Aufwand und Kosten von Dritten nachgeahmt werden können. Auch soll es nicht nachträglich anbringbar, sondern möglichst fester Bestandteil des Produktes sein.
3. Dauerhaftigkeit:
   Das Sicherheitsmerkmal soll während des gesamten Produktlebenszyklus vorhanden und nicht (spurenfrei) entfernbar oder übertragbar auf andere Produkte sein, um eine dauerhafte Authentifizierung zu gewährleisten.
4. Wirtschaftlichkeit:
   Der Einsatz des Sicherheitsmerkmals soll wirtschaftlich sein. Dies beinhaltet auch die einfache Anbringung sowie schnelle und einfache Verifizierbarkeit.

In Abbildung 7 sind Beispiele dieser Integration dargestellt.

Hohlschaftkegel:
Ringetikett mit CDP und 2D-Barcode, bei Ablöseversuch selbstzerstörend

Klammerkette:
Speziallasche mit Kunststoffträger zur Aufnahme eines RFID-Transponders, Kunststoffträger oder Transponder zerstören sich bei Demontageversuch

Siegeldichtung:
Speziallasche zur Aufnahme eines RFID-Transponders, Transponder zerstört sich bei Auslöseversuch aus dem Silikon



Einmesslehre:
RFID-Transponder zerstört sich bei Ablöseversuch

Abbildung 7: Ausgewählte Beispiele von integrierten Sicherheitsmerkmalen aus dem Projekt ProAuthent (Quelle: HOMAG Holzbearbeitungssysteme GmbH, Multivac Sepp Haggenmüller GmbH & Co. KG, VOLLMER WERKE Maschinenfabrik GmbH, Lehrstuhl fml)

5. Errichtung eines Identifikations- und Prüfpunkts

Die Aufbringung von Sicherheitsmerkmalen auf Produkte und Bauteile ist der erste Schritt zur Bekämpfung von Produktpiraterie mit Hilfe von Kennzeichnungstechnologien. Jedoch wird diese Maßnahme erst dann wirksam, wenn die entsprechenden Merkmale beim Weg des Produktes durch die Supply-Chain und insbesondere beim finalen Einsatz geprüft werden [Durchholz et al. 10]. Zur Identifikation und Prüfung der gekennzeichneten Bauteile, sind somit entsprechende Identifikations- und Prüfpunkte (IP-Punkte) notwendig (vgl. auch Abschnitt 6).

An den IP-Punkten wird abhängig von der jeweils verwendeten Kennzeichnungstechnologie mit dem jeweils notwendigen Hilfsmittel das Produkt authentifiziert, d.h. die Originalität des Produktes überprüft. Für die im Projekt relevanten Technologien erfolgt das

- bei RFID mit einem elektromagnetisch arbeitenden Schreib-Lesegerät (SLG)
- bei CDP mit einem optischen Lesegerät
- bei IR-Farben mit einem optischen Lesegerät
- bei Hologramm visuell, d.h. mit dem Auge des qualifizierten Mitarbeiters.

Um Maschinen selbst dazu zu befähigen, eingebaute Teile und Komponenten automatisch auf Originalität zu prüfen, können diese mit den passenden Prüfgeräten ausgerüstet werden. Da die Maschinen und Anlagen meist

ohne Datenverbindung betrieben werden, ist eine besondere Anforderung, dass die Authentifizierung der Originalbauteile ausschließlich lokal mit dem jeweiligen Sicherheitsmerkmal möglich sein muss. Das bedeutet, dass die Prüfung der Echtheit mit den vor Ort verfügbaren Hilfsmitteln durchführbar sein muss. Dies ist für die drei Technologien CDP, IR-Farben, Hologramme intrinsisch gegeben. Für RFID jedoch wurde ein spezielles Verfahren für passive Transponder entwickelt, welches es ermöglicht, Transponder als Sicherheitsmerkmale einzusetzen. Dieses neue Verfahren wird im Folgenden ebenso vorgestellt wie der prinzipielle Aufbau von IP-Punkten am Beispiel von RFID.

An einem IP-Punkt zur Prüfung von Produkten, die mit einem Transponder gekennzeichnet sind, wird ein SLG an einem Rechner angeschlossen. Sobald sich das Produkt im Lesefeld des SLG befindet, werden sämtliche Daten ausgelesen und gemeinsam mit der Reader-Identifikationsnummer (ID) an die verarbeitende Software weitergegeben (vgl. Abbildung 8).
Um das Ergebnis einer Prüfung zu dokumentieren und damit im Nachhinein nachvollziehbar und für weitere Beteiligte der Supply-Chain zugänglich zu machen und auf diesen Daten weitere Prüfungen sowie Funktionen aufbauen zu können, werden bei jedem Prüfvorgang lokale „Daten-Events“ generiert, die eine spezielle Datenstruktur aufweisen und als XML-Datei vorliegen. Die Entstehung der wesentlichen Teile der Dateninhalte dieser XML-Dateien wird in den folgenden Abschnitten dargestellt. Was XML ist, wie die genaue Struktur der XML-Dateien und wie deren Verwendung aussieht, wird in Abschnitt 6 beschrieben.

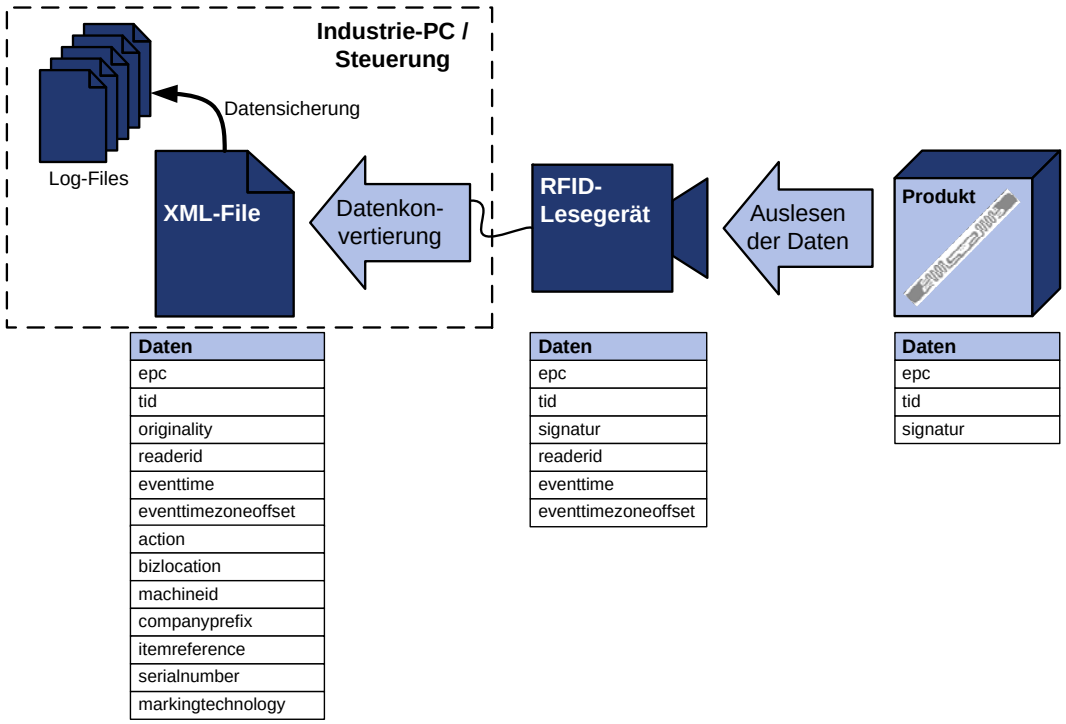


Abbildung 8: IP-Punkt zur Authentifizierung von Produkten, die mit RFID gekennzeichnet sind (Quelle: Lehrstuhl fml)

Bislang beschränkte sich die Nutzung von Verschlüsselungsalgorithmen auf aktive Transponder ([Wildemann 08]). Mit dem im Folgenden dargestellten Verfahren können kryptografische Algorithmen auch für passive Transponder eingesetzt werden.

5.1. Datenmodell für RFID-Transponder

Hierfür müssen auf dem Transponder drei Datenangaben vorhanden sein:

- EPC: Elektronischer Produktcode, weltweit eindeutig identifizierbar [EPCglobal 10]
- TID: Transponder Identnummer bzw. Tag ID, weltweit eindeutig identifizierbar
- Signatur: kryptografisch erzeugter Code, dient der Authentifizierung.

Der EPC und die Signatur werden vom Originalhersteller des Produkts erzeugt und auf den Transponder in den wiederbeschreibbaren Bereich (RW) des Mikrochips geschrieben. Die TID ist eine Nummer, die bereits vom Chiphersteller auf den Mikrochip des Transponders geschrieben wird und sich im sogenannten Read-Only-Bereich (ROM) des Chips befindet.

5.2. Funktion und Erzeugung des EPC und der Signatur

Der EPC identifiziert das jeweilige Produkt weltweit überschneidungsfrei und wird vom Originalhersteller generiert. Im häufigsten Fall handelt es sich dabei um eine SGTIN (Serialized Global Trade Item Number), die der Hersteller nach dem aktuellen EPC Tag Data Standard erstellt [EPCglobal 10] und mit einem geeigneten SLG auf den Transponder schreibt.

Die Signatur auf einem Transponder dient dazu, eine lokale Authentifizierung des Produktes, das den entsprechenden Transponder trägt, vornehmen zu können. Hierfür verschlüsselt der Originalhersteller die Argumente EPC und TID mit Hilfe des privaten Schlüssels eines gewählten asymmetrischen kryptografischen Verfahrens ([Eckert 08], [Schneier 06]) und erzeugt so eine Signatur (vgl. Abbildung 9). Mit Hilfe des SLG wiederum schreibt er diese Signatur auf den Transponder. Der vollständig beschriebene Transponder ist nach den in Abschnitt 4 formulierten Anforderungen als Sicherheitsmerkmal mit dem Produkt manipulationssicher verbunden.

Als kryptografische Verfahren kommen RSA (Rivest, Shamir, Adleman), DSA (Digital Signature Algorithm), ECDSA (DSA auf Elliptischen Kurven), El-Gamal oder Rabin in Frage. Dabei sind insbesondere die Algorithmen DSA und ECDSA zu empfehlen, da diese bei einer IT-technisch/mathematischen Sicherheit bis zum Jahr 2015 nur eine Signaturlänge von 448 Bits benötigen ([Bundenetzagentur 08], [Barker et al. 07], [Malakhov 10]). Dies ist im Falle von RFID mit entscheidend, da auf den Transpondern nur eingeschränkter Speicherplatz zur Verfügung steht.

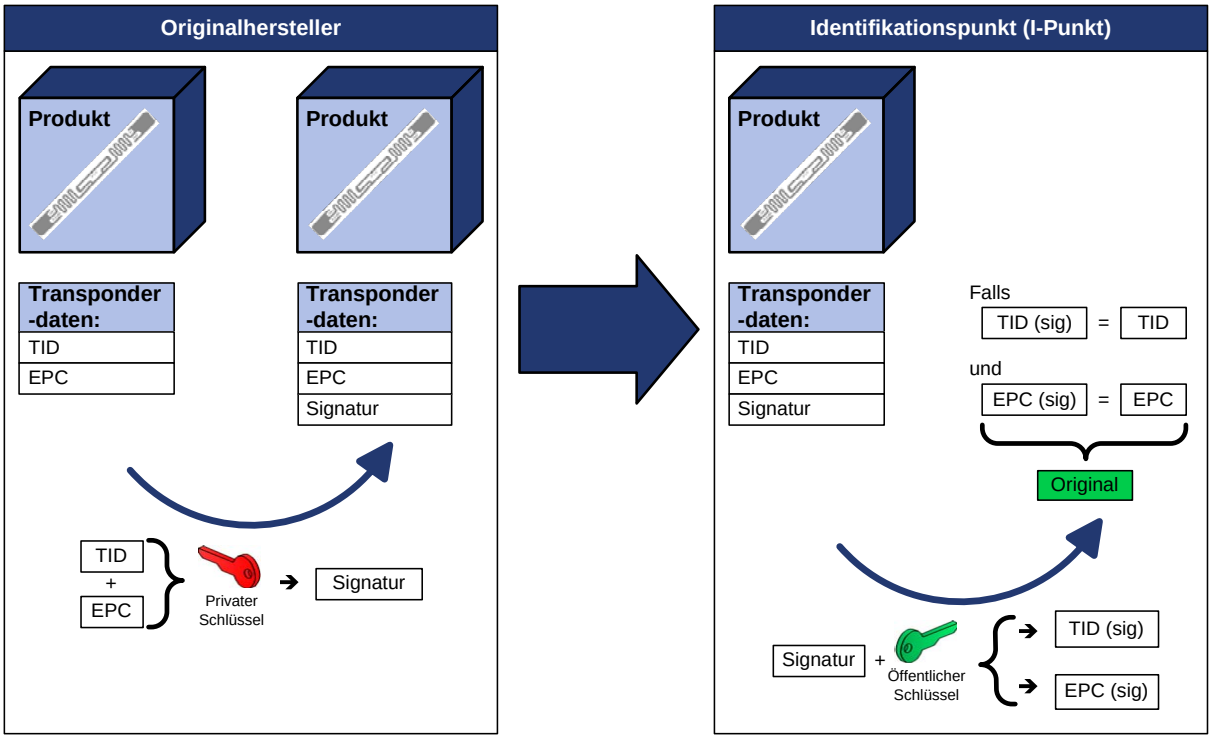


Abbildung 9: Erzeugung und Entschlüsselung einer Signatur (Quelle: Lehrstuhl fml)

5.3. Authentifizierung eines Produkts mittels Signatur

Sobald ein Produkt mit dem signierten Transponder an einem IP-Punkt erfasst wird, werden alle drei Argumente (EPC, TID, Signatur) ausgelesen. Aus der Signatur lassen sich mit Hilfe des passenden öffentlichen Schlüssels die Argumente TID sowie EPC berechnen. Ein Abgleich mit den gelesenen Argumenten weist nach, dass es sich bei Übereinstimmung um ein Originalprodukt handeln muss. Bei Abweichungen handelt es sich entweder um eine Kopie oder ein Originalprodukt, bei dem der EPC oder die Signatur verändert wurden.

5.4. Vor- und Nachteile des RFID-Verfahrens

Der größte Vorteil dieses Verfahrens liegt darin begründet, dass einfache passive und somit preisgünstige Transponder und damit Produkte auf Basis von RFID lokal authentifiziert werden können. Es ist für die Authentifizierung weder ein Online-Zugriff auf eine Datenbank, noch der Einbau aufwändiger Kryptografie-Module in den Transpondern notwendig. Somit können alle vier Anforderungen aus Abschnitt 4 erfüllt werden.

Der Nachteil dieses Verfahrens liegt darin, dass ein Transponder mit einer TID verwendet werden muss, der zusätzlich genügend Speicherplatz für die Signatur bereithält. Außerdem müssen an jedem IP-Punkt der öffentliche Schlüssel zur Entschlüsselung der Signatur und eine Software mit dem entsprechenden Algorithmus zur Verfügung stehen. Da aber für den Betrieb eines SLG ohnehin ein Rechner oder eine Steuerung benötigt wird, kann auf diesem auch die entsprechende Software mit Algorithmus und öffentlichem Schlüssel hinterlegt werden.

6. Integration der IP-Punkte in ein IT-Gesamtsystem

6.1. Aufbau von IP-Punkten und Struktur der XML-Dateien

Ein IP-Punkt kann prinzipiell alle vier in Abschnitt 3 ausgewählten Technologien prüfen (vgl. Abbildung 10). Auch können weitere Technologien hinzugefügt werden. Denn aufgrund der Architektur des IT-Systems und der Nutzung der XML-Datei als Datenschnittstelle ist das Gesamtsystem offen für weitere Technologien.

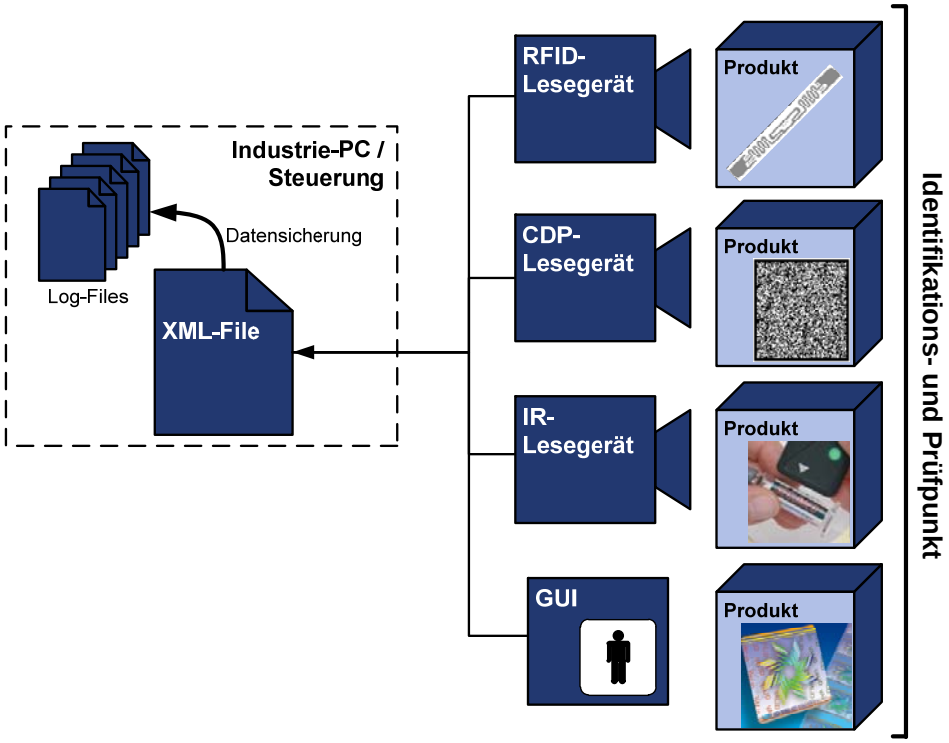


Abbildung 10: Integrierter IP-Punkt für RFID, CDP, IR-Farben und Hologramme (Quelle: Lehrstuhl fml)

Die Auszeichnungssprache XML (Extensible Markup Language) wird zur Darstellung hierarchisch strukturierter Daten in Form von Textdaten genutzt, deren Inhalt unabhängig von der Dokumenttypdefinition ist, d.h. der Inhalt eines XML-Dokumentes kann ohne die Änderung der Struktur geändert werden. XML ist somit ein Standard zur inner- und außerbetrieblichen Informationsübertragung [ten Hompel 06]. Im Forschungsprojekt ProAuthent bildet die XML-Datei das Ergebnis der einzelnen Authentifizierungsvorgänge bzw. der Datenverarbeitung der sicherheitstechnologieindividuellen Software. Dabei ist jede entstehende XML-Datei technologieunabhängig identisch aufgebaut und enthält immer dieselben Elemente. Es sind Angaben zu den Fragen wo, was, wann, warum beinhaltet (in Anlehnung an [EPCglobal 07]):

- EPC: Elektronischer Produktcode
- TID: Transponder Identnummer (die TID kann nur bei der Technologie RFID gespeichert werden)
- Originality: Ergebnis der Originalitätsprüfung
- ReaderID: Seriennummer des Lesegeräts / Name des Prüfers
- Eventtime: Zeitpunkt der Prüfung
- Bizlocation: Ort des Prüfvorgangs
- MachineID: Maschinennummer, an der eine Prüfung durchgeführt werden kann
- Companyprefix: Nummer des Inverkehrbringers
- Itemreference: Sachnummer eines Produktes
- Serialnumber: Fortlaufende Seriennummer für die Produkte gleicher Sachnummer

Je Prüfvorgang wird an jedem IP-Punkt eine XML-Datei, auch als „Event“ bezeichnet, erzeugt.

6.2. Datenübertragung, -hosting und -nutzung

Die je Prüfvorgang an einem IP-Punkt generierten XML-Dateien können in eine zentrale oder dezentrale Datenbank zur weiteren Verarbeitung geladen werden. Hierfür bieten sich SQL-Datenbanken an (Structured Query Language, Standardsprache für relationale Datenbanken [ten Hompel 06]). Die Datenübertragung ist mittels einer Online-Verbindung via Internet oder mithilfe eines Wechseldatenträgers möglich (vgl. Abbildung 11).

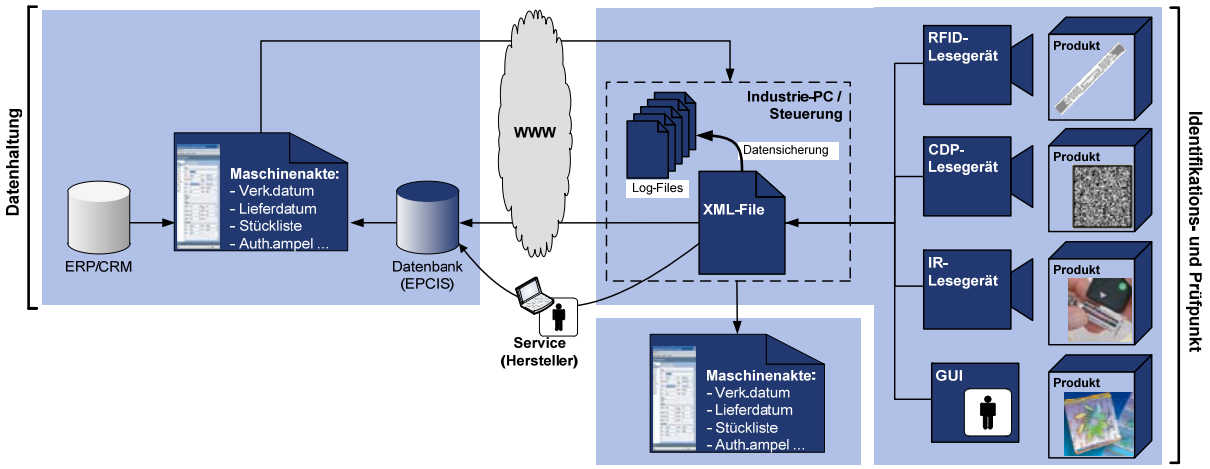


Abbildung 11: IT-Systemarchitektur (Quelle: Lehrstuhl fml)

Basis für die gesamte, für das ProAuthent-Projekt entwickelte IT-Systemarchitektur sowie Datenstruktur bildet der sogenannte EPCIS-Standard (Electronic Product Code Information Services). Dieser Standard ermöglicht es, einer bestimmten vorgegebenen Struktur folgend (de-)zentrale Datenbanken aufzubauen, deren Inhalte von einer zentralen Instanz abgerufen und einem Nutzer zur Verfügung gestellt werden können [EPCglobal 07]. So können sämtliche an IP-Punkten gesammelten Event-Daten in (einer oder mehreren) Datenbanken abgelegt und über diese zentrale Instanz abgefragt werden.

Softwaretechnisch aufbereitet lassen sich daraus für den Nutzer entsprechende Reports erzeugen, die typischerweise als Browserapplikation realisiert sind und Daten aus weiteren unternehmensinternen Datenbanken integrieren können. Da im Forschungsprojekt Bauteile und Komponenten des Maschinen- und Anlagenbaus betrachtet wurden, wurde der Report über die Produkte als „Maschinenakte“ ausgestaltet (vgl. Abbildung 11). Darin sind sämtliche an IP-Punkten gesammelten Daten zu einzelnen Bauteilen einsehbar. Da die Teile final in Maschinen im Einsatz sind, ist auch eine Auflösung der Daten nach der Maschinennummer und somit eine Sicht auf den aktuellen Zustand der ausgewählten Maschine möglich. Die Maschinenakte kann sowohl vom Hersteller der Produkte, vom Maschinenbetreiber oder anderen Beteiligten der Wertschöpfungskette, eingesehen werden.

Zentrales Argument des gesamten Systems ist der EPC, der eine entsprechende Generierung und datentechnische Verknüpfung von Events ermöglicht.

6.3. IP-Punkte zum Schutz des gesamten Wertschöpfungsnetzes

„Zukünftig werden Unternehmen ihre Produkte durch übergreifende und langfristig angelegte Strategien gezielt vor Piraterie schützen müssen. Dazu muss der Produktpirateriesschutz auf die gesamte Wertschöpfungskette ausgeweitet werden.“ [Wildemann et al. 07] Daher werden im Projekt zum Schutz des gesamten Wertschöpfungsnetzes an allen relevanten Stellen IP-Punkte errichtet (vgl. Abbildung 12). Dies ermöglicht einerseits die Produkte auf ihrem Weg durch die Wertschöpfungskette überall zu identifizieren, entsprechende Events zu generieren und somit ein Tracking & Tracing zu realisieren. Andererseits kann so das ganze Original-Netzwerk vor dem Eindringen von Kopien geschützt werden, da diese am IP-Punkt erkannt würden.

Einer der wichtigsten Prüfpunkte sitzt am Ende der Supply-Chain integriert in der Maschine des Kunden. Wenn die Prüfgeräte in der Maschine des Kunden eingebaut und entsprechend angesteuert sind, können Bauteile im eingebauten Zustand vollautomatisch und vor Inbetriebnahme authentifiziert werden. So können eingebaute Kopien erkannt, der Maschinenbetreiber darauf hingewiesen und möglicher Schaden von der Maschine abgewendet werden. Diese Möglichkeit wurde im Forschungsprojekt entwickelt und durch die Realisierung in Pilotinstallationen der beteiligten Anwenderunternehmen validiert.

Wo genau – neben der Integration in die Maschinen selbst – diese IP-Punkte im Wertschöpfungsnetzwerk errichtet werden müssen, ist abhängig von der jeweiligen Organisations-, Beschaffungs- und Vertriebsstruktur der Unternehmen. Meist bietet sich der Wareneingang eines jeden an der Supply-Chain Beteiligten an.

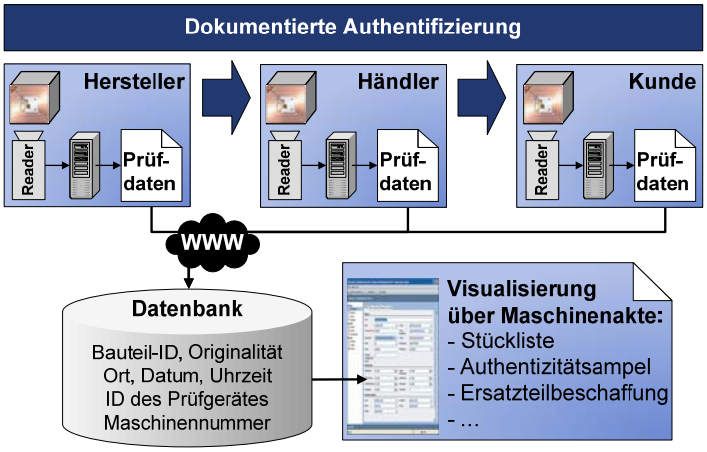


Abbildung 12: IP-Punkte entlang der geschützten Wertschöpfungskette (Quelle: Lehrstuhl fml)

7. Realisierung von Zusatznutzen

Um das Gesamtsystem, wie es in den Abschnitten 5 bis 6 dargestellt ist, wirtschaftlicher gestalten zu können, wurden im Forschungsprojekt sogenannte Zusatznutzen entwickelt und umgesetzt. Dabei wird unter einem Zusatznutzen eine Systemfunktion verstanden, die über die reine Kennzeichnung und Authentifizierung sowie deren Dokumentation hinaus geht. Es gibt Zusatznutzen für den Originalhersteller, den Maschinenbetreiber oder weitere Beteiligte der Supply-Chain, die einen IP-Punkt betreiben. Nach dieser Definition ist die Maschinenakte bereits der erste mögliche Zusatznutzen, der den Teilnehmern Tracking-&-Tracing-Daten über einzelne Bauteile sowie Daten zur aktuellen Maschinenkonfiguration anzeigen kann. Weitere im Forschungsprojekt identifizierte und mit dem ProAuthent-System verknüpf- bzw. realisierbare Zusatznutzen sind in Tabelle 2 und Tabelle 3 gelistet.

Lokal an einem Bauteil / einer Maschine	
Kennzeichen	**Maschinenüberwachung & -reaktion**
• Steigerung der Qualitätsanmutung • Gütesiegel • Gerichtsverwertbarkeit	• Automatische Bauteil-/Werkzeugidentifikation • Verwechslungsschutz für Bauteile und Werkzeuge • Automatische Datenübergabe bauteil- oder werkzeugindividueller Parameter • Selbstkonfiguration bei Originalbauteilen • Signalausgabe: „Alles i.O.“ / Grünes Leuchtsignal • Information ohne / mit Bestätigungserfordernis durch Maschinenbediener • Erstellung bzw. Aktualisierung einer tatsächlichen, realen Maschinenstückliste • Bauteilindividuelle Standzeiterfassung • Protokollierung der Taktzeit / Zyklen des Bauteils in der BDE • Condition-Monitoring • Verschleißerkennung • Information „Verschleißerkennung aktiv“ • Höhere Produktionssicherheit • Ermittlung von Felddaten • Früherkennung von Ausfalltreibern • Serviceampel

Tabelle 2: Lokal an einem Bauteil / in einer Maschine zu realisierende Zusatznutzen (Quelle: Lehrstuhl fml)

Zentral im System		
Ersatzteilmanagemet	**Service**	**Betriebswirtschaft / Marketing**
• Sichere Bestellung und Lieferung von Ersatzteilen • Erleichterte Ersatzteilbeschaffung • Nachverfolgbarkeit der Ersatzteile auf dem Transportweg • Reduzierung der Lagerkosten durch optimales Ersatzteilmanagement mit Just-in-time-Belieferung • Konsignationslager	• Erweiterte Gewährleistungen • Bessere Vorbereitung der Servicetechniker • Verringerung der Dauer der Reaktion im Serviceprozess • jit-Servicemitarbeiter • Service-Priorität „Hoch“: Kunde erhält bevorzugten Service durch OEM • Remote Service (24-7-365) • Fernwartungskonzepte bei Originalteilen durch Einsatz von RFID • Längere Wartungsintervalle • Erleichterte Rückrufaktion • Recycling / Abwrackprämie	• Klassifizierung der Kunden • Bonusprogramme • Kundenwettbewerbe • Einladung zu Produktpräsentationen • Vorführung der Haltbarkeit (Original vs. Konkurrenz) • Zugang zu exklusiven Informationen / Veranstaltungen • Rabatte • Vergünstigte Wartungsverträge • Meldung an lokalen Vertriebspartner bei Kopien für gezieltes Marketing

Tabelle 3: Zentral im System zu realisierende Zusatznutzen (Quelle: Lehrstuhl fml)

8. Juristische Aspekte

Das beschriebene Gesamtsystem wurde durch eine Untersuchung des Lehrstuhl für Wirtschaftsrecht und Geistiges Eigentum der Technischen Universität München juristisch geprüft mit dem Ergebnis:

- Prinzipiell ist das Prüfen von Bauteilen und deren Originalität in Maschinen mit überwachender und beweissichernder Funktion möglich, um ungerechtfertigte Gewährleistungsansprüche abwehren zu können.
- Die Übertragung der gewonnenen Daten in ein zentrales System muss zwischen Maschinenhersteller und Maschinenkäufer/-betreiber vertraglich klar geregelt sein.
- Als zusätzliche Maßnahme können zwischen dem Originalhersteller und dem Maschinenkäufer/-betreiber Alleinbezugsvereinbarungen festgelegt werden, wobei das Wettbewerbsrecht und AGB-Recht berücksichtigt werden muss, vor allem bezüglich der gegenständlichen und zeitlichen Höchstdauer der Bindung.

9. Zusammenfassung

Die im Forschungsprojekt ProAuthent erzielten zentralen Erkenntnisse und wichtigen Ergebnisse lassen sich wie folgt zusammenfassen:

- Von Produktpiraterie betroffene Unternehmen können mit einem methodisch unterstützten Vorgehen schützenswerte Bauteile und passende Kennzeichnungs- und Authentifizierungstechnologien ermitteln (vgl. Abschnitte 2 und 3).
- Zur Kennzeichnung von Ersatzteilen und Komponenten können verschiedene Kennzeichnungstechnologien als Originalitäts- oder Unikatkennzeichen verwendet werden (vgl. Abschnitte 3 und 4).
- Die im Forschungsprojekt ausgewählten bzw. weiterentwickelten Technologien lassen eine lokale Authentifizierung zu, d.h. Prüfung der Echtheit nur an dem jeweiligen Ort und nur mit den dort zur Verfügung stehenden Hilfsmitteln – ohne die Zuhilfenahme weiterer Mittel, wie bspw. ein Online-Datenbank-Abgleich, Laborprüfungen o.ä. (vgl. Abschnitt 5).
- Bei RFID können kostengünstige, passive UHF-Transponder zur lokalen Authentifizierung genutzt werden, sofern das im Forschungsprojekt entwickelte kryptografisch Verfahren zur Erzeugung und Entschlüsselung von Signaturen verwendet wird (vgl. Abschnitte 5.2 und 5.3).
- Zur Dokumentation der Prüfergebnisse können an den IP-Punkten lokal XML-Dateien als „Prüfevent“ erzeugt und in zentral Datenbanken übermittelt werden (vgl. Abschnitt 6)
- Dadurch ist zeitgleich der Aufbau eines Tracking-&-Tracing-Systems möglich, welches das gesamte Wertschöpfungsnetzwerk vor Kopien schützen kann (vgl. Abschnitt 6.3).
- Zur Steigerung der Attraktivität und Wirtschaftlichkeit des Gesamtsystems für den Hersteller und auch Kunden bzw. weitere Beteiligte der Supply-Chain können sowohl lokal an den einzelnen IP-Punkten

sowie zentral auf dem Datenbanksystem aufbauend sogenannte Zusatznutzen eingerichtet werden (vgl. Abschnitt 7)
- Das gesamte entwickelte ProAuthent-System zur Kennzeichnung und Authentifizierung von kritischen Bauteilen im Maschinen- und Anlagenbau als integrierter Produktpiraterieschutz kann in Maschinen übertragen werden (vgl. Abschnitt 5).
- Das System ist juristisch geprüft und bei entsprechender vertraglicher Regelung vollständig rechtskonform (vgl. Abschnitt 8).

Es konnte somit erstmalig ein System zur Kennzeichnung und dokumentierten Authentifizierung schützenswerter Bauteile des Maschinen- und Anlagenbaus entwickelt, in einem Demonstrator aufgebaut und in Pilotinstallationen der Anwenderunternehmen umgesetzt werden. Den Unternehmen dieser Branche steht damit ein System zur Verfügung, um Komponenten und Ersatzteile mit Sicherheitsmerkmalen zu kennzeichnen sowie zuverlässig von Kopien unterscheidbar zu machen und das gesamte Wertschöpfungsnetzwerk vor dem Eindringen von Kopien zu schützen. Dabei ist es insbesondere möglich, Maschinen und Anlagen so auszustatten, dass diese selbständig in der Lage sind, die Originalität der eingebauten Teile zu überprüfen. Die Umsetzbarkeit des Systems in der Realität konnte ebenso gezeigt werden, wie dessen rechtliche Zulässigkeit.
Das ProAuthent-System ermöglicht es den Unternehmen, Bauteile und Komponenten, mit technischen Mitteln präventiv vor Produktpiraterie zu schützen.

Literatur

[3S Simons 11] 3S Simons Security Systems GmbH: Secutag®. Bilder und Bildrechte von ARIADNE MedienAgentur, Redaktion Public Relations, Sandra Appel, 24.08.2011

[Abele et al. 10] Abele, E.; Albers, A.; Aurich, J.; Günthner, W. (Hrsg.): Wirksamer Schutz gegen Produktpiraterie im Unternehmen – Piraterierisiken erkennen und Schutzmaßnahmen umsetzen. Band 3 der Reihe „Innovationen gegen Produktpiraterie“.VDMA Verlag GmbH, Frankfurt a. M., 2010

[Alien Technology 11] Alien Technology Corporation: ALN-964X Squiggle® Inlay. Bild und Bildrechte von Alien Technology, Direction of Marketing, Neil Mitchell, 24.08.2011

[Barker et al. 07] Barker, E.; Barker, W.; Burr, W.; Polk, W.; Smid, M.: Computer Security. Recommendation for Key Management Part 1: General. National Institute of Standards and Technology, Gaithersburg, 2007

[Bundesministerium des Inneren 05a] Bundesministerium des Inneren: Weiterentwicklung der Fälschungssicherheit von Pässen und Personalausweisen. Bundesdruckerei GmbH, Berlin, 2005

[Bundesministerium des Inneren 05b] Bundesministerium des Inneren: Das Indentigramm. Ein neues Sicherheitsmerkmal für Pässe und Personalausweise. Bundesdruckerei GmbH, Berlin, 2005

[Bundenetzagentur 08] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung – Übersicht über geeignete Algorithmen. Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Mainz, 2008

[Chip Online 04] Chip Online: Nokia bietet Internet-Prüfung für Handy-Akkus. http://www.chip.de/news/Nokia-bietet-Internet-Pruefung-fuer-Handy-Akkus_12801306.html. CHIP Xonio Online GmbH, München, 2004
Letzter Aufruf: 14.04.2011

[Durchholz et al. 10] Durchholz, J.; Stockenberger, D.; Günthner, W.A.: Dokumentierte Authentifizierung als wirksamer Schutz vor Produktpiraterie für Komponenten im Maschinen- und Anlagenbau. In: 6. Fachkolloquium der WGTL e.V., Tagungsband, S. 245-254. Wissenschaftliche Gesellschaft für Technische Logistik e.V., Stuttgart, 2010

[Eckert 08] Eckert, C.: IT-Sicherheit. Konzepte, Verfahren, Protokolle. Oldenbourg, München, 2008

[EPCglobal 07] EPCglobal: EPC Information Services (EPCIS) Version 1.0.1 Specification.

EPCglobal, Brüssel 2007

[EPCglobal 10] EPCglobal: EPC Tag Data Standard Version 1.5. EPCglobal, Brüssel, 2010

[Günthner et al. 08] Günthner, W.; Durchholz, J.; Meißner, S.; Stockenberger, D.: Potenziale des Produktpirateriesschutzes durch kognitive Authentifizierung. In: Industrie Management 6/2008, S.23. Gito, Berlin, 2008

[Halbach 11] Diagramm Halbach GmbH & Co. KG: http://www.halbach.com/index.html. Letzter Aufruf: 14.04.2011

[ICC 06] ICC – International Chamber of Commerce: Anti-counterfeiting technology – A guide to Protecting and Authenticating Products and Documents. ICC, Barking (GB), 2006

[Malakhov 10] Malakhov, E.: Anwendung kryptografischer Verfahren zur Authentifizierung von RFID-Tags. fml – Lehrstuhl für Fördertechnik Materialfluss Logistik, Garching, 2010

[Mitsubishi HiTec Paper 11] Mitsubishi HiTec Paper Flensburg GmbH: Innovation für den Alltag – Papier & Sicherheit. www.mitsubishi-paper.com. Letzter Aufruf: 14.04.2011

[Nokia Corporation 11] Nokia Corporation: Nokia Standard-Akku BL-4C. Bild und Bildrechte von Nokia Corporation, Anne Beringer, 25.08.2011

[Pipimaru 11] Pipimaru: http://commons.wikimedia.org/wiki/Category:Rail_tickets_of_the_Deutsche_Bahn?uselang=de. Letzter Aufruf: 14.04.2011

[Schneier 06] Schneier, B.: Angewandte Kryptographie. Protokolle, Algorithmen und Sourcecode in C. Pearson Studium, München, 2006

[Schreiner Group 11] Schreiner Group: Markenschutz in Gips gegossen. http://www.schreiner-prosecure.de/index.php?id=639&L=0 Letzter Aufruf: 14.04.2011

[ten Hompel 06] Ten Hompel, M.: Taschenlexikon Logistik. Abkürzungen, Definitionen und Erläuterungen der wichtigsten Begriffe aus Materialfluss und Logistik. Springer, Berlin, 2006

[VDMA 10] VDMA: VDMA-Umfrage zur Produkt- und Markenpiraterie 2010. VDMA, Frankfurt a.M., 2010

[Völcker 06] Völcker, T.: Einsatz innovativer Sicherheitstechnologien für den effektiven Produkt- und Markenschutz. http://www.muenchen.ihk.de/mike/ihk_geschaeftsfelder/recht/Anhaenge/Vortrag-Schutz-mit-Sicherheitstechnologie.pdf. Letzter Aufruf: 22.08.2011

[von Welser 07] Von Welser, M.; González, A.: Marken- und Produktpiraterie. Strategien und Lösungsansätze zu ihrer Bekämpfung. Wiley-VCH, Weinheim, 2007

[Wildemann et al. 07] Wildemann, H.; Ann, C.; Broy, M.; Günthner, W.A.; Lindemann, U.: Plagiatschutz – Handlungsspielräume der produzierenden Industrie gegen Produktpiraterie. TCW, München, 2007

[Wildemann 08] Wildemann, H.: Produktpiraterie. Leitfaden zur Einführung eines effizienten und effekiven Kopierschutz-Managements. TCW, München, 2008

[Winkler, Wang 07] Winkler, I.; Wang, X.: Made in China – Marken- und Produktpiraterie. Strategien der Fälscher & Abwehrstrategien für Unternehmen. Verlag für Interkulturelle Kommunikation, Frankfurt a.M., London 2007

Abkürzungen

CRM	Customer Relationship Management
EPC	Elektronischer Produktcode
ERP	Enterprise Resource Planning
fml	Lehrstuhl für Fördertechnik Materialfluss Logistik der Technischen Universität München
HSK	Hohlschaftkegel
ID	Identifikationsnummer
IP-Punkt	Identifikations- und Prüfpunkt
IT	Informationstechnik
PC	Personal Computer
RFID	Radiofrequenz-Identifikation
CDP	Copy Detection Pattern
IR	Infrarot-Farbpigmente
ROM	Read-Only-Memory
RW	ReWritable-Memory
SLG	Schreib-Lesegerät
SQL	Structured Query Language
TID	Transponder Identnummer
UV	Ultraviolett-Farbpigmente
XML	Extensible Markup Language

Abbildungen

Tabellen