Schlussbericht für das Forschungsprojekt ProAuthent

Integrierter Produktpiraterieschutz durch Kennzeichnung und Authentifizierung von kritischen Bauteilen im Maschinen- und Anlagenbau

Günthner, W. A. – Durchholz, J. – Stockenberger, D.

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

BETREUT VOM

PTKA Projektträger Karlsruhe im Karlsruher Institut für Technologie

Dieses Forschungs- und Entwicklungsprojekt wurde mit Mitteln des Bundesministeriums für Bildung und Forschung (BMBF) im Rahmenkonzept „Forschung für die Produktion von morgen“ gefördert und vom Projektträger Karlsruhe (PTKA) betreut.
Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

Inhaltsverzeichnis

1 Aufgabenstellung

Das Ziel im Forschungsprojekt ProAuthent ist die Entwicklung eines umfassenden, präventiv wirkenden Produktpiraterieschutzsystems für Unternehmen des Maschinen- und Anlagenbaus. Mit einer fälschungssicheren, technischen Lösung soll die Überprüfung der Echtheit von Komponenten und Bauteilen durch Kennzeichnung und Authentifizierung entlang der Wertschöpfungskette aber auch beim Einsatz in Maschinen und Anlagen zum Schutz vor dem Einbau von Kopien mit ihren schädlichen Folgen möglich sein. Das Kennzeichen selbst wird zur Erhöhung der Fälschungs- und Manipulationssicherheit in die Produkte und Komponenten eingebracht und ermöglicht während der gesamten Lebensdauer eine Authentifizierung des Originals. Bei der methodisch unterstützten Auswahl von passenden Kennzeichnungstechnologien werden die technischen Rahmenbedingungen bei der Herstellung und am Einsatzort sowie die Anforderungen aus Kundensicht berücksichtigt.

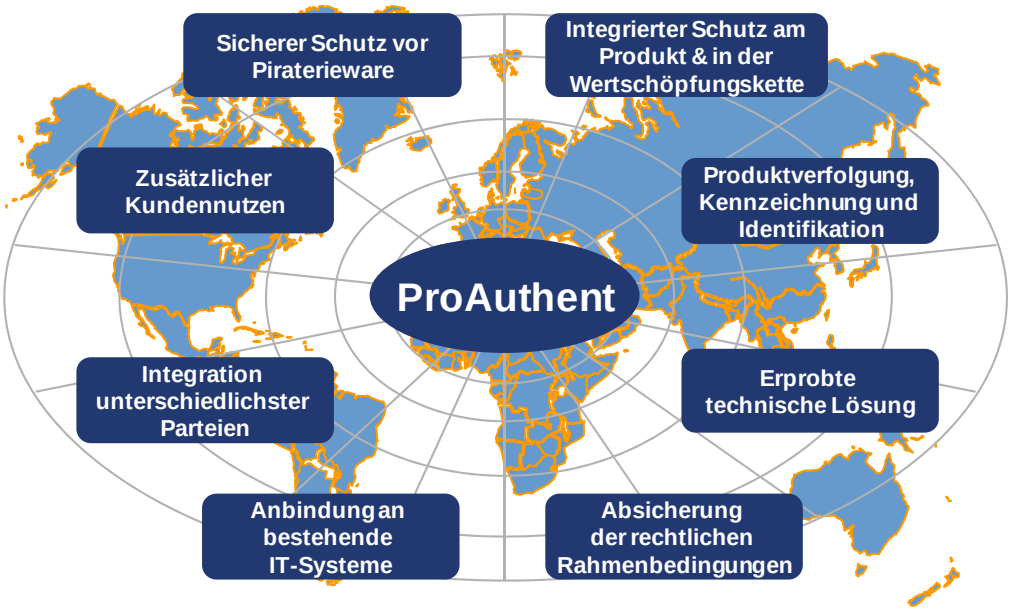


Abbildung 1: Ziele des Forschungsprojektes ProAuthent

Die durchgängige Verfolgung der Originalbauteile über die gesamte Wertschöpfungskette bis zum Einbau stellt eine übergreifende Echtheitstransparenz für die Beteiligten der Supply Chain (Hersteller, Händler, Kunden, …) her. Das hierfür verwendete IT-System kann bereits existierende und gängige IT-Systeme (ERP, CRM etc.) anbinden und somit hochintegrierte Daten zu den jeweiligen Produkten zur Verfü-

gung stellen. Zur Erhöhung der Attraktivität und Wirtschaftlichkeit des Gesamtsystems werden neue Dienstleistungen und Produktfunktionalitäten entwickelt, welche zusätzlichen Nutzen für den Hersteller, den Kunden sowie weitere Beteiligte der Supply Chain erzeugen. Somit entsteht eine wirtschaftliche Lösung für die betroffenen Unternehmen, die in Produkte und Prozesse integriert werden kann. Hierfür müssen die unternehmensübergreifenden Prozesse und Schnittstellen gestaltet werden:

- wo, wann und wie wird das Bauteil gekennzeichnet,
- wie werden Kontroll- und Steuerungsinstanzen in der Wertschöpfungskette ausgestaltet und etabliert,
- wie können die Teilnehmer der Supply Chain die Ware selbstständig und dezentral auf Originalität prüfen.

Nach Auswahl der passenden Kennzeichnungstechnologien und Entwicklung des IT-gestützten Systems sowie der neuen Zusatznutzen und Dienstleistungen erfolgt die Prüfung juristischer Aspekte sowie die rechtliche Zulässigkeit des Gesamtsystems, das anschließend in vorwettbewerblichen Pilotinstallationen umgesetzt wird (vgl. Abbildung 1).

Insgesamt kann mit dem IT-gestützten System zur Authentifizierung der Originalprodukte das Einschleusen von gefälschten Komponenten und Ersatzteilen in die Wertschöpfungskette sowie deren Inbetriebnahme in Maschinen und Anlagen verhindert werden. Die durch Produktpiraterie bedingten Schäden werden durch dieses präventiv wirkende, technische System auf ein Minimum reduziert. Gleichzeitig erhöht sich durch neue Produktfunktionalitäten und Zusatznutzen die Wettbewerbsfähigkeit der Unternehmen.

2 Voraussetzungen für die Durchführung des Vorhabens

Das Gesamtbudget des **fml** - Lehrstuhl für Fördertechnik Materialfluss Logistik der Technischen Universität München betrug 437.200 €. Zur Bearbeitung des Projektes wurden 66 Mensch-Monate für jeweils einen Mitarbeiter sowie zwei wissenschaftliche Hilfskräfte mit einem Betrag von 366.960 € gefördert. An Sachkosten wurde ein Budget von 56.240 €, für Reisen 14.000 € zur Verfügung gestellt. Somit konnte das Projekt während nahezu der gesamten Laufzeit von zwei wissenschaftlichen Mitarbeitern sowie der genannten Anzahl an wissenschaftlichen Hilfskräften bearbeitet werden. Die am Lehrstuhl fml vorhandenen Einrichtungen zum Test von RFID-Systemen sowie diverses RFID-Equipment wurden im Projekt genutzt sowie um die notwendigen Ausrüstungsgegenstände für spezielle Untersuchungen sowie den Aufbau eines Demonstratorsystems aus den Sachmitteln erweitert.
Im Projekt konnte das Wissen aus der Erarbeitung der Studie „Plagiatschutz – Handlungsspielräume der produzierenden Industrie gegen Produktpiraterie“ eingebracht und genutzt werden (vgl. Abbildung 2). Darin sind neben den durch Produktpiraterie entstehenden volkswirtschaftlichen und betriebswirtschaftlichen Schäden und der Handlungsweise von Produktpiraten insbesondere die existierenden Ansätze und Methoden gegen Produktpiraterie aus Produktgestaltung und Konstruktion, Produktion und Produktionstechnologie, IT-Sicherheit, Betriebswirtschaft sowie juristische Mittel sowie existierende Defizite und Lücken aufgezeigt [Wil-07].

Abbildung 2: Plagiatschutz – Handlungsspielräume der produzierenden Industrie gegen Produktpiraterie [Wil-07]

Aus gestarteten und teilweise parallel laufenden weiteren Forschungsprojekten des Lehrstuhl fml wurden inhaltliche Impulse und Erkenntnisse in das Forschungsprojekt ProAuthent getragen. Beispielsweise „RFID in der Logistik – Werkzeuge zur Identifikation und Nutzung von RFID Potenzialen“ (Bayerische Forschungsstiftung). Darin wurden Fragestellungen zu Einsatzbereichen von RFID (Wareneingang, Warenausgang, Lagerverwaltung etc.) und mit RFID unterstützbare Funktionen (Inventuren, Bestandskontrollen, Wareneingangskontrollen etc.) evaluiert und für RFID-Anwender aufbereitet. Insbesondere das gesammelte und vorhandene Know-how zu am Markt verfügbaren RFID-Komponenten sowie technischen Testmethoden ermöglichten eine schnelle Orientierung hinsichtlich dieser Auto-ID-Technologie [FML-11a]. Aus dem Forschungsprojekt „Transparenter Prototyp“ (INI.TUM-Projekt) wurden Konzepte zur durchgängigen und konsistenten Datenhaltung mit Hilfe geeigneter Identifikationstechnologien aufgegriffen und verarbeitet [FML-11b]. Auch das im Projekt „RFID-Einsatz in der Baubranche“ (AiF-FV 15288 N/1) gesammelte Wissen hinsichtlich dem technischen Einsatz von RFID, dem Aufbau mobiler Identifikationspunkte, der datentechnischen Einbindung und dem Aufbau entsprechender Daten- und Kommunikationsstrukturen (vgl. Abbildung 3) konnte sehr gut transferiert und genutzt werden [FML-11c].

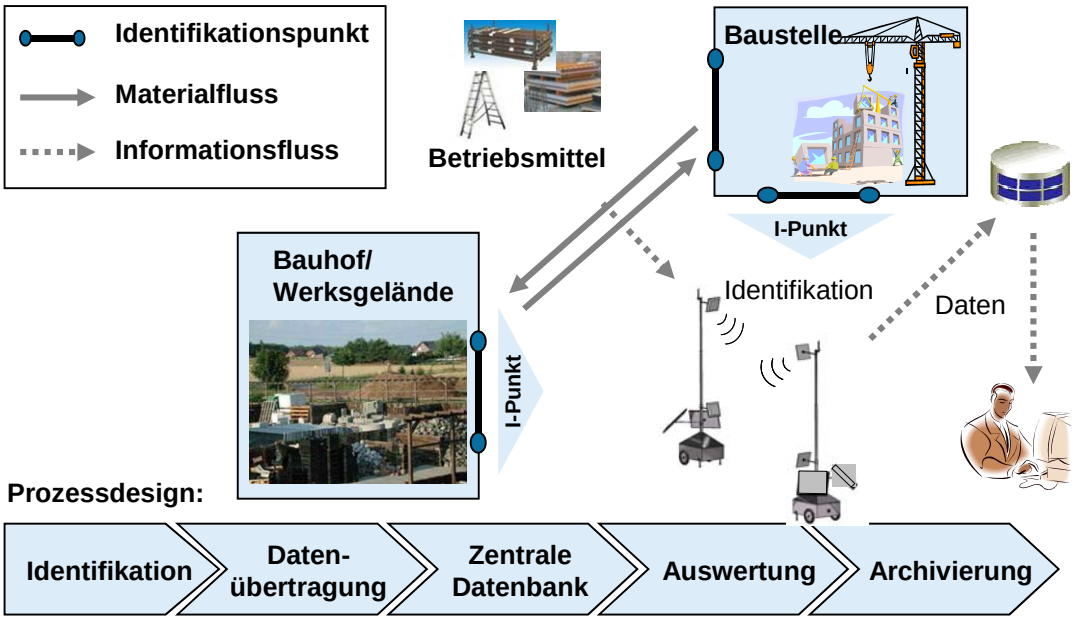


Abbildung 3: Material- und Informationsfluss bei der Verfolgung von Betriebsmitteln in der Baubranche [FML-11c]

Somit reiht sich das Projekt ProAuthent logisch in die strategische Entwicklung des LS fml ein. Dabei werden folgende Ziele und Aktivitäten verfolgt:

- Entwicklung innovativer RFID-Anwendungen
- Ausbau des Forschungsgebiets „Integration von RFID in Objekte“
- Aufbau des Forschungsgebiets „Smart Objects“

- Aufbau des Forschungsgebiets „Materialflusssteuerung und Automatisierung durch Auto-ID-Technologien“
- Aufbau des Forschungsgebiets „Datensynthese – Vom Reader zum Anwender“
- Ausweitung des Forschungsgebiets „Methodik zur Prozessgestaltung mit RFID“
- Aufbau des Forschungsfeldes „Auto-ID-Technologien allgemein“

Das im Juni 2010 gestartete Forschungsprojekt FORFood TP6 „Sichere und effiziente Supply Chain in der Lebensmittelindustrie durch einen intelligenten Behälter“ (Bayerische Forschungsstiftung) kann auf die in ProAuthent erarbeiteten Konzepte und das methodische Vorgehen aufbauen. Die Ausrüstung von Kühlbehältern mit sensorisch bestückten RFID-Transpondern soll ein Tracking & Tracing sowie Temperaturerfassung und -übertragung in Echtzeit ermöglichen. Das Datenmodell lehnt sich dabei an das ProAuthent-IT-System an.

3 Wissenschaftlicher und technischer Stand zu Beginn und Ende des Vorhabens

Produktpiraterie- und Kopierschutz sind vielfältig aus dem Alltag und prominenten Beispielen bekannt (vgl. Abbildung 4). Diese werden unter anderem auf Verpackungen eingesetzt, welche von Konsumenten als erstes wahrgenommen werden und die Kaufentscheidung beeinflusst. Zur fälschungssicheren Gestaltung gibt es vielfältige Möglichkeiten der Verpackungsabsicherung sowie Sicherheitstechnologien die von Malik/Schindler als „Produktschutzarsenal“ ([Mal-05] S.8) bezeichnet und ausführlich beschrieben werden. [Mal-05]
Im Bereich des Maschinen- und Anlagenbaus jedoch 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“ ([Wil-07] S.8). Dabei ist das Erkennen der Piraterieware eine Grundlage der wirksamen Bekämpfung von Produktpiraterie. Die Kopien von Bau- und Ersatzteilen erreichen oftmals ein so hohes Qualitätsniveau, dass die Identifikation der Piraterieware schwierig ist ([Wil-07], S.56, vgl. Abbildung 5). Um den Schutz von Originalbauteilen und -produkten zu gewährleisten, gibt es verschiedene Möglichkeiten ([Wil-07], S.56):

- durch Produktkennzeichnung und -authentifizierung
- durch Verfolgung und Überwachung der Produkte
- durch 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 [Bun-05]

Fahrkarten, Eintrittskarten und Tickets:

Sicherheitsmerkmale wie spezielle Einfärbungen, Hologramme, Wasserzeichen, UV-fluoreszie-rende Fasern etc. ([Hal-11], [Mit-11], [Com-11])

Handy-Akkus der Nokia GmbH:

Hologramm ([Chi-04], [Nok-09] S.12)

Baustoffe der Knauf Gips KG:

Sicherheitsmarkierung mit Hologramm, thermoreaktive Farbe ([Sch-11], [Völ-06])

Sportartikel der PUMA AG:

Textiletiketten mit Mikrofarbcodes ([Sim-11], [Wel-07] S. 334)

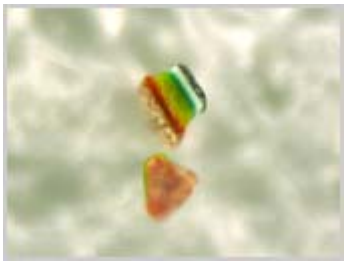


Abbildung 4: Verschiedene Sicherheitstechnologien in diversen Produkten und prominenten Beispielen

Abbildung 5: Original und Kopie [Quelle: APM - Aktionskreis gegen Produkt- und Markenpiraterie e.V.]

Wildemann et al. stellen in ihrer Studie „Plagiatschutz – Handlungsspielräume der produzierenden Industrie gegen Produktpiraterie“ im Jahr 2007 folgende Punkte als offenen Forschungsbedarf fest:

- Sichere Kennzeichnung von Produkten:
  Neben existierenden Auto-ID-Verfahren „fehlen derzeit die notwendigen Voraussetzungen in Form von fälschungssicheren Produktkennzeichnungen“ ([Wil-07], S.62 f.).
- Identifizierungs- und Verifizierungssysteme sowie deren Einbettung in vorhandene IT-Systeme:
  Zur durchgängigen Produktverfolgung müssen Identifizierungs- und Verifizierungs-systeme entwickelt und eingerichtet sowie mit existierenden ERP- und SCM-Systemen verknüpft werden ([Wil-07], S.62 f.)
- Bauteilverifizierung an Maschinen und Anlagen:
  Maschinen und Anlagen müssen mit eigener „Prüfintelligenz“ ausgestattet werden, so dass diese die Bauteilverifizierung durch eine Online-Verbindung aber auch dezentral und „offline“ durchführen können ([Wil-07], S.76 f.).

Dieser Forschungsbedarf wurde im Forschungsprojekt ProAuthent aufgegriffen. Während der Bearbeitung des Projektes haben sich die genannten Lücken bestätigt und wurden, wie ab Abschnitt 3.1 dargestellt, erarbeitet.

Wie in Abbildung 6 erkennbar ist, sind im deutschen Maschinen- und Anlagenbau 62% der befragten Unternehmen von Produktpiraterie betroffen. Das Ausmaß des wirtschaftliche Schadens durch Produktpiraterie beträgt laut Schätzung des VDMA in der zugrundeliegenden Studie etwa 6,4 Mrd € pro Jahr – dieser Umsatz würde der Branche ca. 40.000 Arbeitsplätze sichern. Dabei sind zunehmend Komponenten und Ersatzteile betroffen. [VDMA-10]

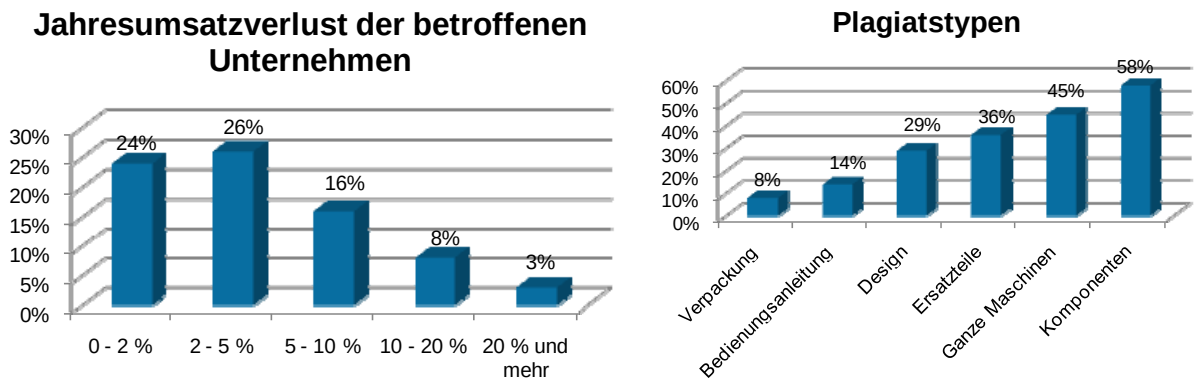


Abbildung 6: Kennzahlen zur Produktpiraterie im deutschen Maschinen- und Anlagenbau [VDMA-10]

Zum Schutz von Ersatzteilen und Komponenten des Maschinen- und Anlagenbaus wurde daher im Forschungsprojekt ProAuthent ein integrierter Produktpirateriesschutz durch Kennzeichnung und Authentifizierung entwickelt. Dabei wurde am Lehrstuhl fml ein methodisches Vorgehen gewählt, das in den nächsten Abschnitten beschrieben wird und gleichzeitig das validierte und empfohlene Vorgehen für Unternehmen darstellt, die ihre Produkte durch Kennzeichnung und Authentifizierung vor Produktpiraterie schützen wollen. Dabei konnten die als oben Forschungsbedarf genannten Punkte aufgegriffen und erarbeitet werden. Maßgeblich für den Aufbau eines Produktpiraterie-Abwehrsystems sind die folgenden Schritte:

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.

3.1 Auswahl von schützenswerten Bauteilen

In Unternehmen des Maschinen- und Anlagenbaus sind vor allem lukrative Komponenten und Ersatzteile betroffen ([Gün-08], [Wil-07] S.4, [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. Dabei haben sich im Forschungsprojekt ProAuthent die in Abbildung 7 gelisteten Kriterien zur Auswahl der schützenswerten Bauteile bewährt.

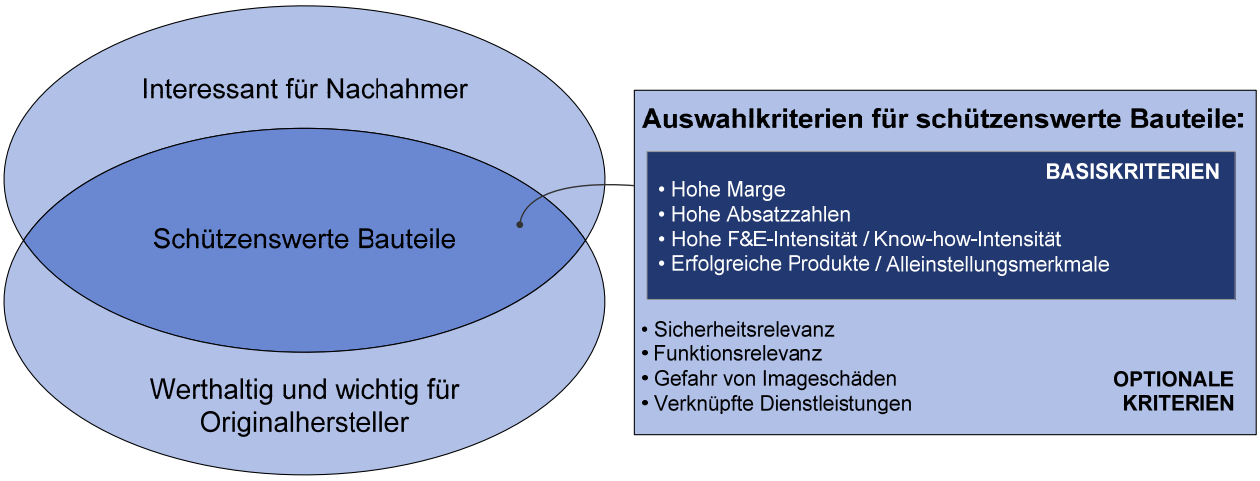


Abbildung 7: Kriterien zur Auswahl der schützenswerten Bauteile

Dabei entsprechen die schützenswerten Bauteile immer den Basiskriterien. Weitere Bauteile können identifiziert werden, wenn die optionalen Kriterien zusätzlich herangezogen werden. Auf dieser Basis wurden bei den Anwenderunternehmen die in Abbildung 8 dargestellten Teile als schützenswert ermittelt.

Abbildung 8: Schützenswerte Bauteile der Anwenderunternehmen

3.2 Auswahl passender Kennzeichnungstechnologien

Nach Bestimmung der schützenswerten Bauteile muss eine Auswahl der je Bauteil passenden Kennzeichnungstechnologie erfolgen. Vor der Nutzung eines kopiersicheren Sicherheitsmerkmals, 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 9). ([Wil-08] S.74)

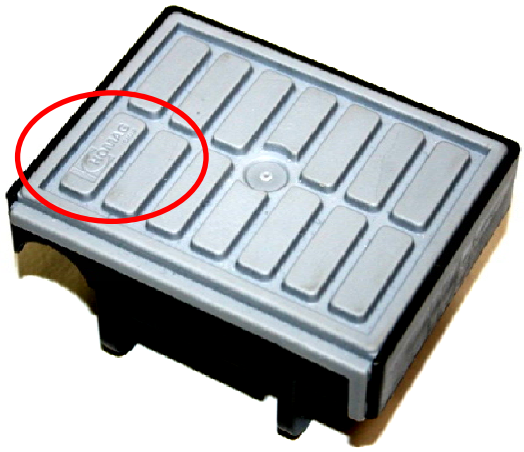


Abbildung 9: Bauteil mit Firmenlogo: Kettenplatte der HOMAG Holzbearbeitungssysteme GmbH

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 dessen späteren Kennzeichens aufgenommen. Diese lassen sich in technische (vgl. Abbildung 10) sowie betriebswirtschaftliche (vgl. Abbildung 11) Einflussgrößen gliedern.

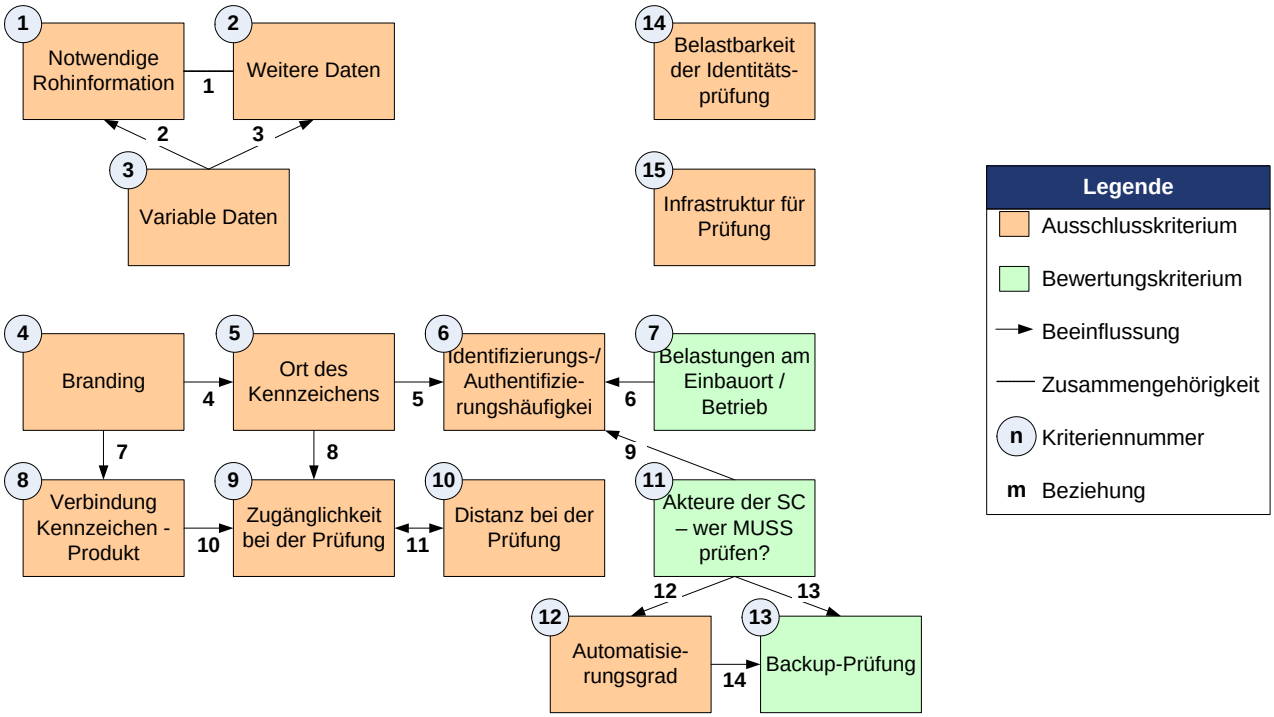


Abbildung 10: Technische Einflussgrößen

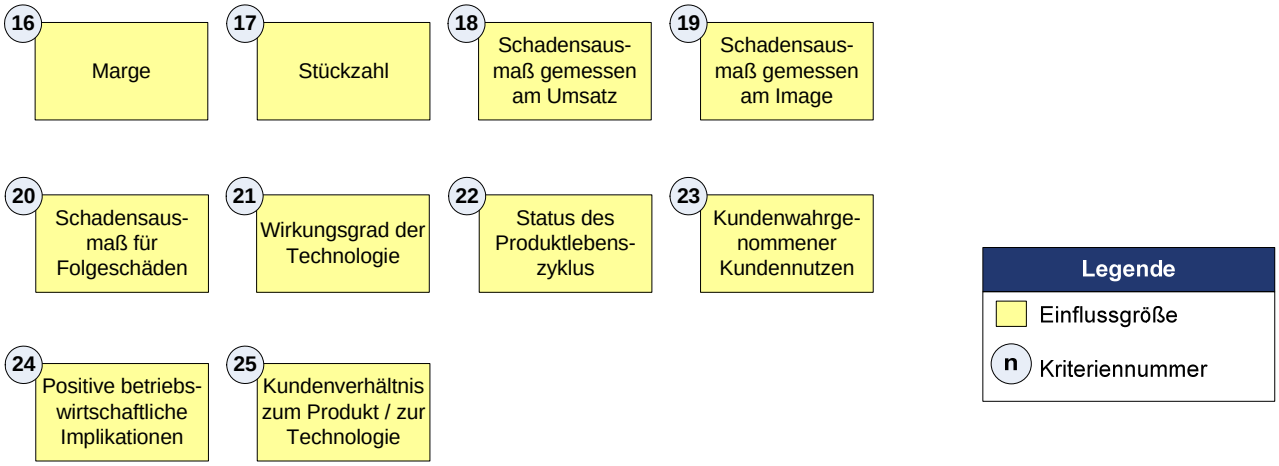


Abbildung 11: Betriebswirtschaftliche Einflussgrößen

Diese Einflussgrößen wurden im Forschungsprojekt genau definiert und deren Ausprägungen für die 31 gelisteten Kennzeichnungstechnologien (vgl. Tabelle 1) erarbeitet. Da die resultierende Tabelle mit allen Ausprägungen je Technologie mehrere Seiten füllt, wird diese hier nicht als Abbildung eingefügt. Wichtig ist jedoch der folgende Mechanismus. Über die Ausprägungen der Einflussgrößen je schützenswertem Bauteil sowie die Ausprägungen der Einflussgrößen je Kennzeichnungstechnologie lässt sich die größtmögliche Übereinstimmung zwischen Bauteil und Kennzeichnungstechnologie 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

Das Ergebnis dieser Auswahl für die beteiligten Anwenderunternehmen ist in Abbildung 12 zu sehen. Es wurden somit die folgenden vier Kennzeichnungs- und Authentifizierungs-technologien als die in den analysierten Fällen des Maschinen- und Anlagenbaus beste Technologien bestimmt (vgl. Abbildung 13):

1. RFID (Radiofrequenz-Identifikation):
   Auto-ID-Technologie, deren Transponder (Mikrochip mit Antenne zur (elektro-) magnetischen Kopplung) mit Schreib-Lesegeräten berührungslos erfassbar, auslesbar und beschreibbar sind.
2. CDP (Copy Detection Pattern):
   Gedrucktes Rauschmuster das nicht kopierbar und mit optischen Lesegeräten authentifizierbar ist
3. IR-Farben (Infrarot):
   Farbpigmente, die mit Lesegeräten detektierbar und aufgrund der im Einzelfall spezifischen Farbmischung kopiersicher sind.
4. Hologramm:
   Aufwendig erzeugte Abbildungen, die bei Beleuchtung mit gleichartigem Licht ein dreidimensionales Abbild eines Gegenstands erscheinen lassen und nicht kopierbar sind.

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 (vgl. [Wil-07] S.64 f.). Weitere Eigenschaften der vier

Technologien wurden steckbriefartig zusammengetragen und veröffentlicht – hier sind diese Tabellen in Tabelle 2 und Tabelle 3 zu sehen.

Diese am LS fml in Zusammenarbeit mit dem im Projekt beteiligten Lehrstuhl BWL entwickelte Methodik zur Auswahl passender Kennzeichnungstechnologien lässt sich zukünftig auch auf andere Unternehmen übertragen und anwenden.

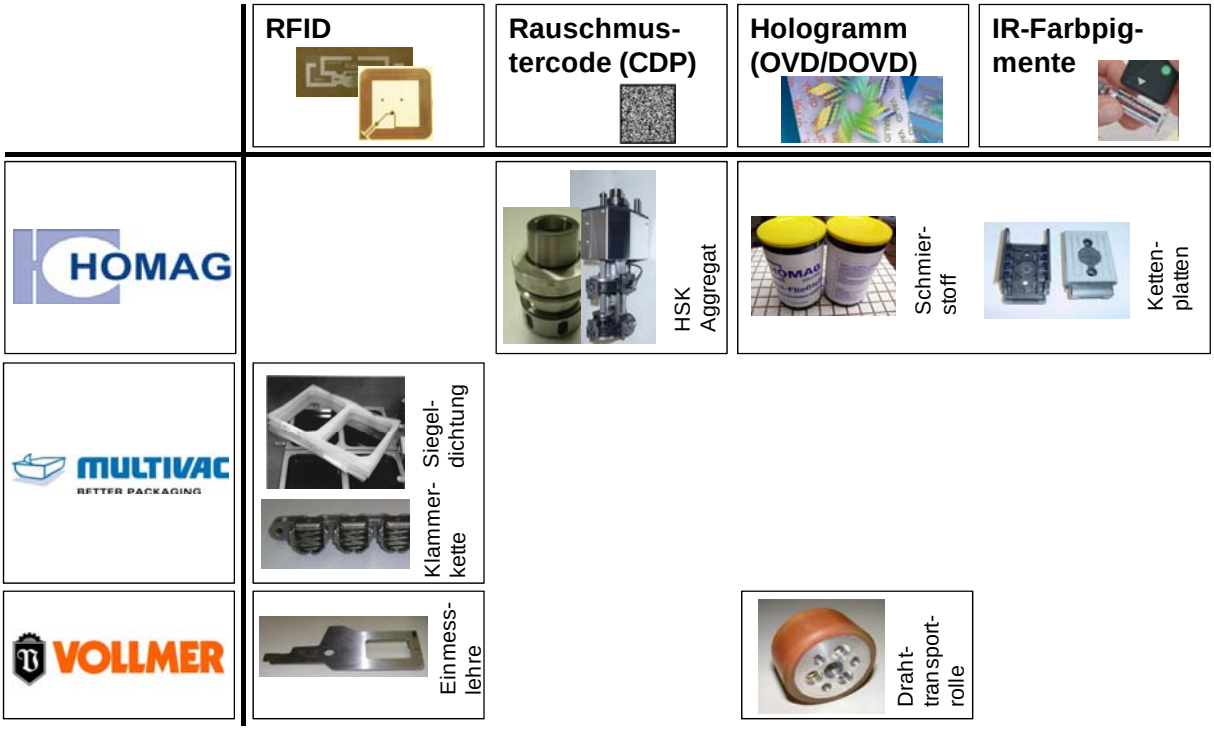


Abbildung 12: Kennzeichnungstechnologie je schützenswertem Bauteil der Anwenderunternehmen

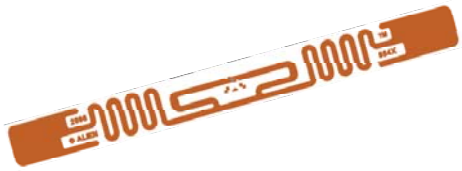
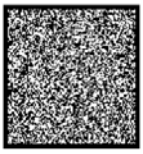
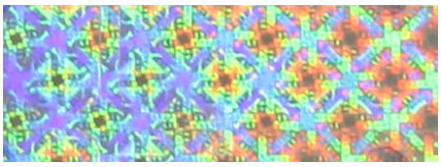
RFID: UHF-Transponder der Firma Alien Technology Corporation: ALN-9640 Squiggle® Inlay [Ali-10]	
CDP: Copy Detection Pattern der Fa. Schreiner CDP-Rauschmuster	
IR: IR-Klebeetikett der Firma Schreiner Group GmbH & Co. KG – die IR-Farbpigmente sind für das menschliche Auge unsichtbar	
Hologramm: Hologramm der Firma Schreiner Group GmbH & Co. KG als Druckvorlage (li.) sowie als Klebeetikett (re.)	 

Abbildung 13: Kennzeichnungstechnologie je schützenswertem Bauteil der Anwenderunternehmen

Radiofrequenz-Identifikation (RFID)	
Stufe	Unikatkennzeichen
Kennzeichen	Transponder: IC mit Antenne zur (elektro-)magnetischen Kopplung
Trägermaterial	Verschiedenste Formen (Label, Hard Tag etc.)
Grundmaterial	Frequenzabhängig, Schwierigkeiten bei leitfähigen Materialien
Ort	Etikett auf Produkt oder Verpackung, integriert in Produkt oder Verpackung etc.
Kennzeichnung / Applikation	Aufkleben, Eingießen etc.
Prüfung / Identifizierung	Antenne, Lesegerät, Rechner / Steuerung
Prüf- / Identifizierungs-häufigkeit	Unbegrenzt
Wirkprinzip der Prüfung	Elektromagnetisch
Kontakt bei Prüfung	Berührungsfrei
Kopiersicherheit	Abhängig vom konkreten System: Klonen von Transpondern mit EPC einfach; Klonen von Transpondern mit EPC und UID sehr schwer
Manipulationssicher-heit	Ablösen des Transponders von der Befestigung abhängig. Zerstörung des Transponders durch mechani-sche Einflüsse möglich
Robustheit	Negativer Einfluss von leitfähigen Materialien (Metall, Flüssigkeiten) auf Lesbarkeit; Schutz des Transponder-Inlays vor mechani-schen Einflüssen notwendig
Typisches Einsatzgebiet	Logistik, Werkzeugerkennung, Schließsysteme etc.
Arten / Ausprägungen	Verschiedene Systeme (z. B. Frequenzen, Standards etc.)
Speichermöglichkeit / -art	Digitale Daten auf Mikrochip
Speichergröße	Bis mehrere hundert kBytes
Speicherbeschreibbar-keit	Einmalig oder wiederbeschreibbar
Erkennungswert beim Kunden, Kommunikati-onsaufwand	Informationen sind nur mit speziellen Lesegeräten auslesbar

Copy Detection Pattern (CDP)	
Stufe	Unikatkennzeichen
Kennzeichen	Gedrucktes Rauschmuster
Trägermaterial	Bedruckbare, laserbeschriftbare Materialien
Grundmaterial	Wie Trägermaterial; beliebig bei Verwendung eines Etiketts
Ort	Produkt, Verpackung
Kennzeichnung / Applikation	Direkt Bedrucken, Aufbringen eines Etiketts, Laserbeschriftung
Prüfung / Identifizierung	Scanner, spezielles Lesegerät
Prüf- / Identifizierungs-häufigkeit	Unbegrenzt
Wirkprinzip der Prüfung	Optisch
Kontakt bei Prüfung	Berührungsfrei
Kopiersicherheit	Hoch
Manipulationssicher-heit	Mechanisch zerstörbar, Übertragung muss durch geeignete Applikation verhindert werden.
Robustheit	Abhängig von der Applikation
Typisches Einsatzgebiet	Banknoten, Dokumente
Arten / Ausprägungen	CDP, BitSecure, Speicherung von zusätzlichen Daten im Rauschmus-ter möglich
Speichermöglichkeit / -art	Binäre Daten
Speichergröße	In Abhängigkeit von der Größe des Musters (z. B. 96 bit)
Speicherbeschreibbar-keit	Einmalig bei der Erzeugung des Musters
Erkennungswert beim Kunden, Kommunikati-onsaufwand	Offenes Merkmal, spezielle Prüfgeräte notwendig

Tabelle 2: Eigenschaften von RFID und CDP (Quelle [Abe-11] S.47 f.)

Infrarotfarben	
Stufe	Originalitätskennzeichen
Kennzeichen	Farbpigmente (evtl. mit Trägermaterial)
Trägermaterial	Folie, Etikett, Bindemittel / Lack, keines etc.
Grundmaterial	Beliebig
Ort	Verpackung, Etikett, Banknote
Kennzeichnung / Applikation	Aufkleben, Drucken, Lackieren, etc.
Prüfung / Identifizierung	Manuelle / elektronische IR-Prüfgeräte
Prüf- / Identifizierungs-häufigkeit	Unbegrenzt
Wirkprinzip der Prüfung	Optisch
Kontakt bei Prüfung	Berührungsfrei
Kopiersicherheit	Beschaffung von IR-Farbpigmenten schwierig
Manipulationssicher-heit	Evtl. mechanisch entfernbar
Robustheit	Abhängig vom Trägermaterial, sehr robust
Typisches Einsatzgebiet	Banknoten, Medikamentenver-packungen
Arten / Ausprägungen	IR-Farbe verschiedener Wellen-längen
Speichermöglichkeit / -art	Keine
Speichergröße	-
Speicherbeschreibbar-keit	-
Erkennungswert beim Kunden, Kommunikati-onsaufwand	Verdecktes Merkmal, manuelle Prüfung mit einfachsten Handlese-geräten
Anmerkung	Sicherheitsniveau abhängig von Kombination und Codierung unterschiedlicher Pigmente

Hologramme / Optically Variable Device (OVD)	
Stufe	Originalitätskennzeichen
Kennzeichen	Hologramm / Hologramm(folie)
Trägermaterial	Folien, Etiketten
Grundmaterial	Beliebig (als Etikett) oder direkt auf Kunststoff
Ort	Verpackung, Etikett
Kennzeichnung / Applikation	Aufkleben oder in Spritzgussform integrieren
Prüfung / Identifizierung	Einfache optische Prüfung; eingehende optische Prüfung von bestimmter Merkmale mit Mikroskop
Prüf- / Identifizierungs-häufigkeit	Unbegrenzt
Wirkprinzip der Prüfung	Optisch
Kontakt bei Prüfung	Berührungsfrei
Kopiersicherheit	Hologramme sind nicht reproduzierbar. Wesentlich ist immer die eingehende Prüfung.
Manipulations-sicherheit	Mechanisch zerstörbar, abhängig von der Art der Applikation
Robustheit	Widerstandsfähig, limitierte UV-Stabilität
Typisches Einsatzgebiet	Medizinprodukte, Verpackungen, Banknote
Arten / Ausprägungen	2D- und 3D-Hologramme
Speichermöglichkeit / -art	In der Regel keine (bei TesaHolospot: Einbringen einer Nummer möglich)
Speichergröße	(Sonderlösungen: bis 1024 Bit)
Speicherbeschreibbar-keit	(Sonderlösungen: einmalig)
Erkennungswert beim Kunden, Kommunikati-onsaufwand	Offenes Merkmal, einfache optische Prüfung. Eingehende optische Prüfung durch Experten.

Tabelle 3: Eigenschaften von IR-Farben und Hologrammen (Quelle [Abe-11] S.45 f.)

3.3 Integration der Kennzeichen in die schützenswerten Bauteile

Die Integration der identifizierten passenden Kennzeichnungstechnologien in die betrachteten Bauteile (vgl. Abbildung 12) erfolgte im Forschungsprojekt schwerpunktmäßig bei den Anwenderunternehmen (Homag, Multivac, Vollmer), so dass diese Inhalte in den Abschlussberichten der Projektpartner ausführlich und daher hier nur kurz dargestellt sind. In Abbildung 14 ist das Ergebnis zu sehen. Ziel der Integration der Sicherheitsmerkmale war es, den folgenden für alle Installationen dieser Art grundlegenden Anforderungen zu genügen (in Anlehnung an [ICC-06], [Win-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.

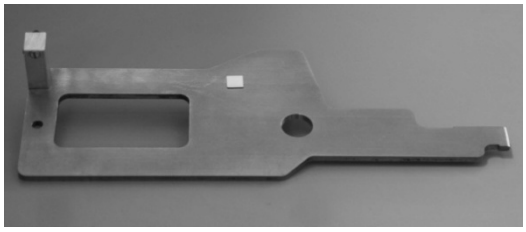
	Homag, Hohlschaftkegel: Ringetikett mit CDP und 2D-Barcode, bei Ablöseversuch selbstzerstörend
	Multivac, Klammerkette: Speziallasche mit Kunststoffträger zur Aufnahmen eines RFID-Transponders, Kunststoffträger oder Transponder zerstören sich bei Demontageversuch
	Multivac, Siegeldichtung: Speziallasche zur Aufnahme eines RFID-Transponders, Transponder zerstört sich bei Auslöseversuch aus dem Silikon
	Vollmer, Einmesslehre: RFID-Transponder zerstört sich bei Ablöseversuch

Abbildung 14: Ausgewählte Beispiele von integrierten Sicherheitsmerkmalen aus dem Projekt

3.4 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 [Dur-10]. Zur Identifikation und Prüfung der gekenn-

zeichneten Bauteile, sind somit entsprechende Identifikations- und Prüfpunkte (IP-Punkte) notwendig (vgl. auch Abschnitt 3.5).

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 in diesem Forschungsprojekt relevanten Technologien erfolgt das

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

Dies wird für die einzelnen Technologien in den folgenden Abschnitten genauer beschrieben. Dabei war im Projekt eine besondere Anforderung, dass eine Authentifizierung von Produkten ausschließlich lokal mit dem jeweiligen Sicherheitsmerkmal möglich sein muss. Das bedeutet, dass die Prüfung der Echtheit mit den dort zur Verfügung stehenden Hilfsmitteln durchführbar sein muss – ohne die Zuhilfenahme weiterer Mittel, wie bspw. ein Online-Datenbank-Abgleich, Laborprüfungen o.ä.

Um das Ergebnis der 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 aussieht und wie deren Verwendung aussieht, wird in Abschnitt 3.5 beschrieben.

3.4.1 IP-Punkt für 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 16).

Für die im Forschungsprojekt ProAuthent existierende maßgebliche Forderung der lokalen Authentifizierung der Objekte wurde ein spezielles Verfahren für passive

Transponder entwickelt, das eine neue Handlungs- und Anwendungsoption im Bereich von RFID eröffnet. Bislang beschränkte sich die Nutzung von Verschlüsselungsalgorithmen auf aktive Transponder ([Wil-08] S.106). Mit dem im Folgenden dargestellten Verfahren können kryptografische Algorithmen auch für passive Transponder eingesetzt werden.

3.4.1.1 Datenmodell für RFID

Hierfür müssen auf dem Transponder drei Datenangaben vorhanden sein (vgl. Abbildung 16):

- EPC: Elektronischer Produktcode, weltweit eindeutig identifizierbar ([EPC-10] S.15, [Fin-06] S.311)
- 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.

3.4.1.2 Funktion und Erzeugung des EPC und der Signatur

er 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 [EPC-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 asymmetrischen kryptografischen Verfahrens ([Eck-08] S.317, [Sch-06]) und erzeugt so eine Signatur (vgl. Abbildung 15). Mit Hilfe des SLG wiederum schreibt er diese Signatur auf den Transponder. Der vollständig beschriebene Transponder wird nach den in Abschnitt **Fehler! Verweisquelle konnte nicht**

gefunden werden. formulierten Anforderungen als Sicherheitsmerkmal mit dem Produkt manipulationssicher verbunden.

Als kryptografische Verfahren kommen in Frage:

- RSA (benannt nach den Erfindern Rivest, Shamir, Adleman)
- DSA (Digital Signature Algorithm)
- ECDSA (DSA auf Elliptischen Kurven)
- El-Gamal
- Rabin

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 ([Bun-08] S.4, [Bar-07] S.37 f., [Mal-10] S.17). Dies ist im Falle von RFID mit entscheidend, da auf den Transpondern nur eingeschränkter Speicherplatz zur Verfügung steht.

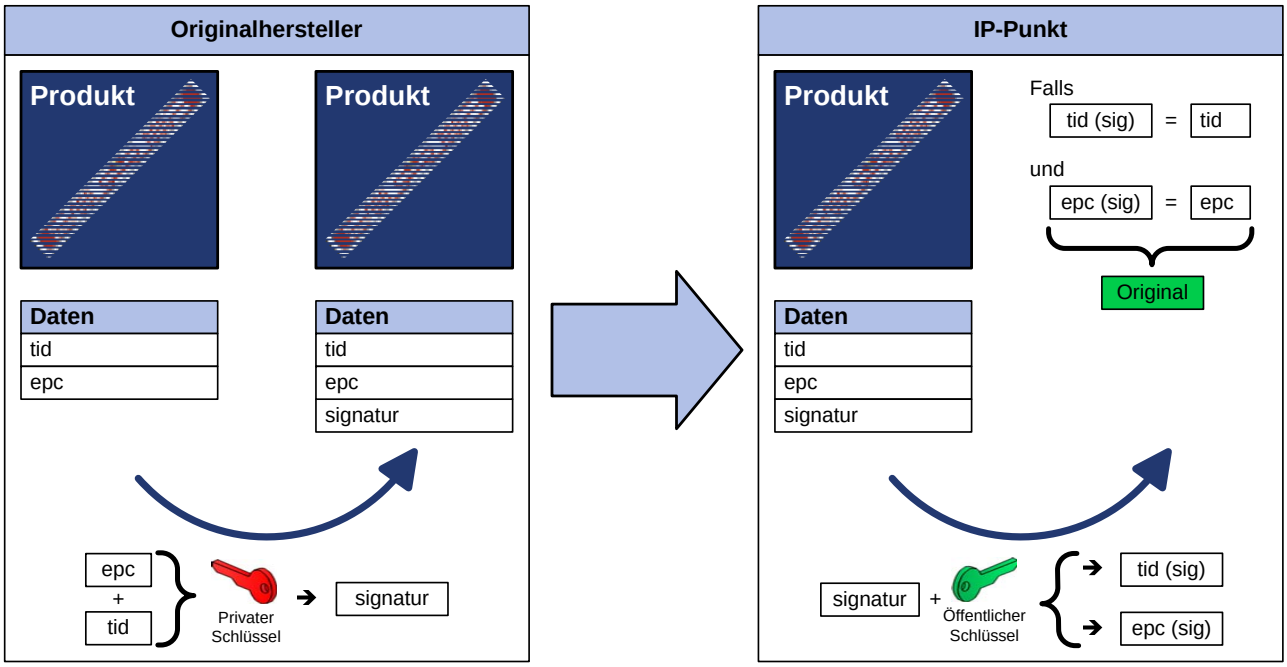


Abbildung 15: Erzeugung und Entschlüsselung einer Signatur

3.4.1.3 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 (vgl. Abbildung 16, Abbildung 17). Aus der Signatur lassen sich mit Hilfe des passenden öffentlichen

Schlüssels die Argumente TID sowie EPC berechnen (vgl. Abbildung 15). 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.

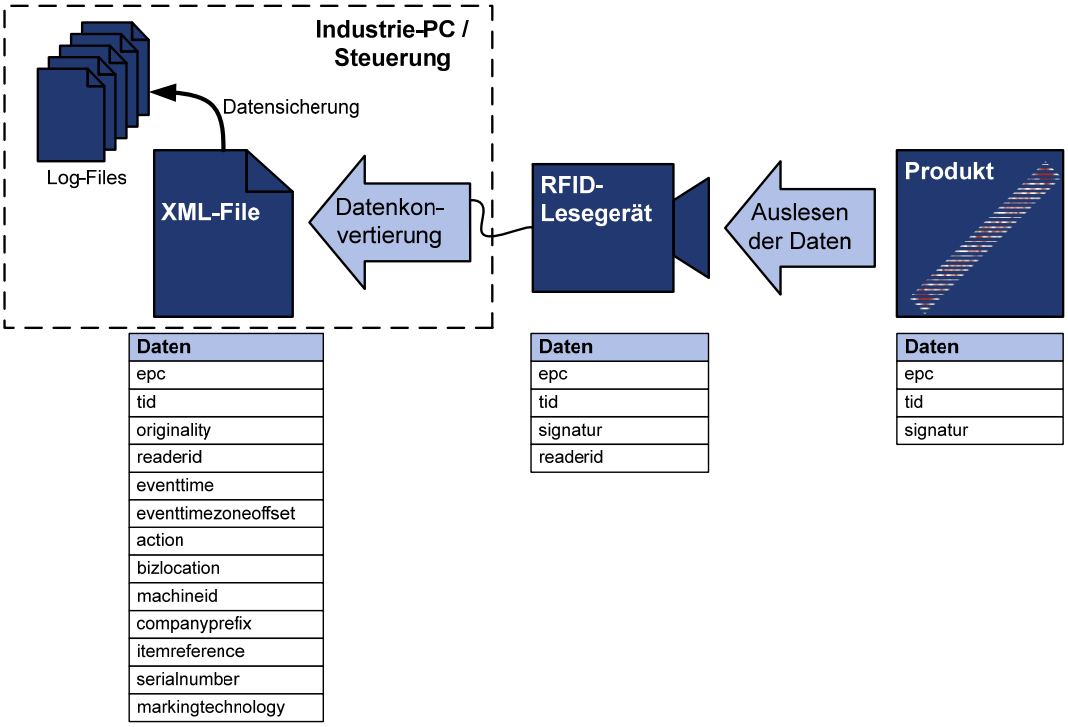


Abbildung 16: IP-Punkt zur Authentifizierung von Produkten, die mit RFID gekennzeichnet sind

Abbildung 17: Realisierung eines IP-Punkt am Demonstrator des Lehrstuhl fml zur Authentifizierung von Produkten, die mit RFID gekennzeichnet sind

3.4.1.4 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. Damit 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 **Fehler! Verweisquelle konnte nicht gefunden werden.** 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.

3.4.2 IP-Punkt für CDP

An einem IP-Punkt, an dem mit CDP gekennzeichnete Produkte auf Originalität geprüft werden sollen, muss ein entsprechendes Lesegerät zur Verfügung stehen, das zur Dokumentation der erfassten Daten an einen Rechner angeschlossen sein soll. Sobald ein CDP auf einem Produkt erkannt wird, wird dieses vom Lesegerät ausgewertet und die erzeugten Daten zusammen mit der ID an die verarbeitende Software weitergegeben (vgl. Abbildung 18).

3.4.2.1 Datenmodell für CDP

Die Forderung der lokalen Authentifizierung kann im Falle des CDP leicht erfüllt werden, da es sich in diesem Fall um ein optisches Rauschmuster handelt, in dessen Druckbild Daten im Umfang von mehreren Bytes gespeichert werden können [Vor-09]. Somit können in einem CDP zwei Daten direkt oder indirekt vorhanden sein (vgl. Abbildung 18):

- EPC: Elektronischer Produktcode, weltweit eindeutig identifizierbar ([EPC-10] S.15, [Fin-06] S.311)
- Originalität.

Der EPC wird zum Zeitpunkt der Erzeugung des CDP vom Originalhersteller des Produkts generiert und im Rauschmuster codiert.

3.4.2.2 Funktion und Erzeugung des EPC und des CDP

Wie in Abschnitt 3.4.1.2 dient auch in diesem Fall der EPC zur weltweit überschneidungsfreien Identifikation des jeweiligen Produkts und wird vom Originalhersteller erzeugt. Im Falle des CDP kann der EPC in das Rauschmuster codiert und mit dem Muster auf das Produkt aufgebracht werden. Dabei sind verschiedene Verfahren wie aufkleben manipulationssicherer Etiketten, aufdrucken, auflasern etc. denkbar.

3.4.2.3 Authentifizierung mittels CDP

Die Originalität des CDP und damit des jeweiligen Produktes wird dadurch ermittelt, dass das Rauschmuster mit einem optischen LG erfasst und mit dem im LG hinterlegten digitalen Abbild des CDP, dem sogenannten CDP-Profil verglichen wird (vgl. Abbildung 18, Abbildung 19). Unterschreitet die Qualität des gescannten Bilds einen empirisch bestimmten Schwellwert nicht, handelt es sich um ein Original, andernfalls um eine Kopie. Denn mit jedem Druck bzw. Scan und erneutem Druck ist ein Qualitätsverlust verbunden, der durch keine existierende Drucktechnik vermieden und durch dieses Verfahren detektiert werden kann. Nach der Feststellung der Originalität wird aus dem CDP der EPC entschlüsselt.

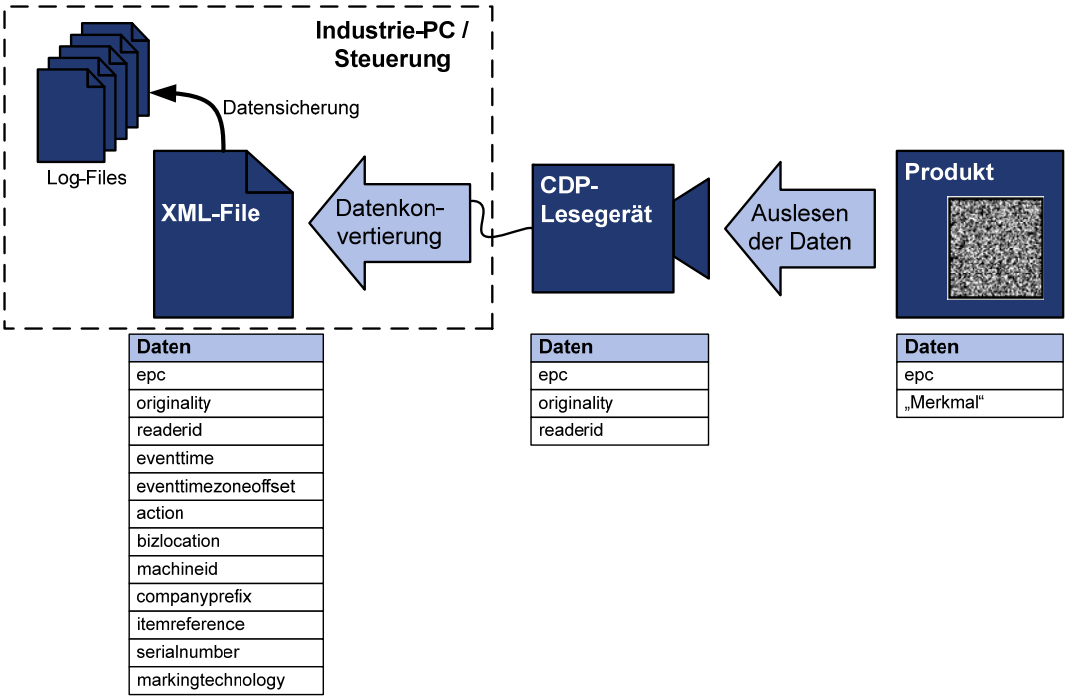


Abbildung 18: IP-Punkt zur Authentifizierung von Produkten, die mit CDP gekennzeichnet sind

Abbildung 19: Realisierung eines IP-Punkt am Demonstrator des Lehrstuhl fml zur Authentifizierung von Produkten, die mit CDP gekennzeichnet sind

3.4.2.4 Vor- und Nachteile des CDP-Verfahrens

Der Vorteil dieses Verfahrens liegt darin begründet, dass CDPs auf Produkte mittels Laserbeschriftung und somit manipulationssicher aufgebracht werden können. Auch ist mit diesem Verfahren eine lokale Authentifizierung möglich. Somit sind alle vier Anforderungen aus Abschnitt **Fehler! Verweisquelle konnte nicht gefunden werden.** erfüllt.

Der Nachteil dieses Verfahrens liegt darin, dass das CDP empfindlich gegenüber Verschmutzung und abrasiven Prozessen ist (Kratzer, Abrieb etc.) und dass die Erkennung nur mit speziellen Lesegeräten bzw. Kameras und spezieller Software mög-

lich ist. Auch muss das CDP in einem sehr stabilen Prozess erzeugt werden, da sonst die Qualität des Druckbildes zu stark schwankt.

3.4.3 IP-Punkt für IR-Farben

An einem IP-Punkt zur Prüfung von Produkten, die mit IR-Farbe gekennzeichnet sind, wird ein LG an einem Rechner angeschlossen. Da es sich bei IR-Farben aber um ein Originalitätskennzeichen handelt, ist die datentechnische Erfassung und Verarbeitung des Prüfergebnisses nicht, wie bei RFID oder CDP, gänzlich automatisch möglich. Zwar kann die Originalität mit Hilfe eines IR-LG detektiert werden, eine automatische Erfassung eines EPC ist damit jedoch nicht möglich.

3.4.3.1 Datenmodell für IR-Farben, Erzeugung und Authentifizierung mittels IR-Farben

Die lokale Authentifizierung von IR-Farben ist leicht möglich, weil in der IR-Farbmarkierung einzig die Originalität in Form von „Farbe vorhanden“ oder „Farbe nicht vorhanden“ codiert ist. Diese Ja-Nein-Aussage ist somit das einzige Argument, das codiert wird:

- Originalität.

Hierfür wird vom Originalhersteller eines Produktes eine IR-Farbmarkierung an der dafür vorgesehenen Stelle des Produktes aufgebracht.

Zur Authentifizierung eines Produktes wird dieses mit der IR-Farbmarkierung vor den Sensor des LG gebracht und die Farbe detektiert (vgl. Abbildung 20, Abbildung 21). Entspricht diese dem erwarteten Farbprofil und ist in der notwendigen Konzentration vorhanden, schließt man auf die Originalität des Produktes. Das Ergebnis kann von der Software des angeschlossenen Rechners verarbeitet werden.

Ein EPC kann nicht gleichzeitig mit der IR-Farbe codiert werden. Dieser muss mit Hilfe eines anderen Kennzeichens (1D-/2D-Barcode, Klarschrift o.ä.) am Produkt angebracht und dem Rechner automatisch oder manuell übergeben werden.

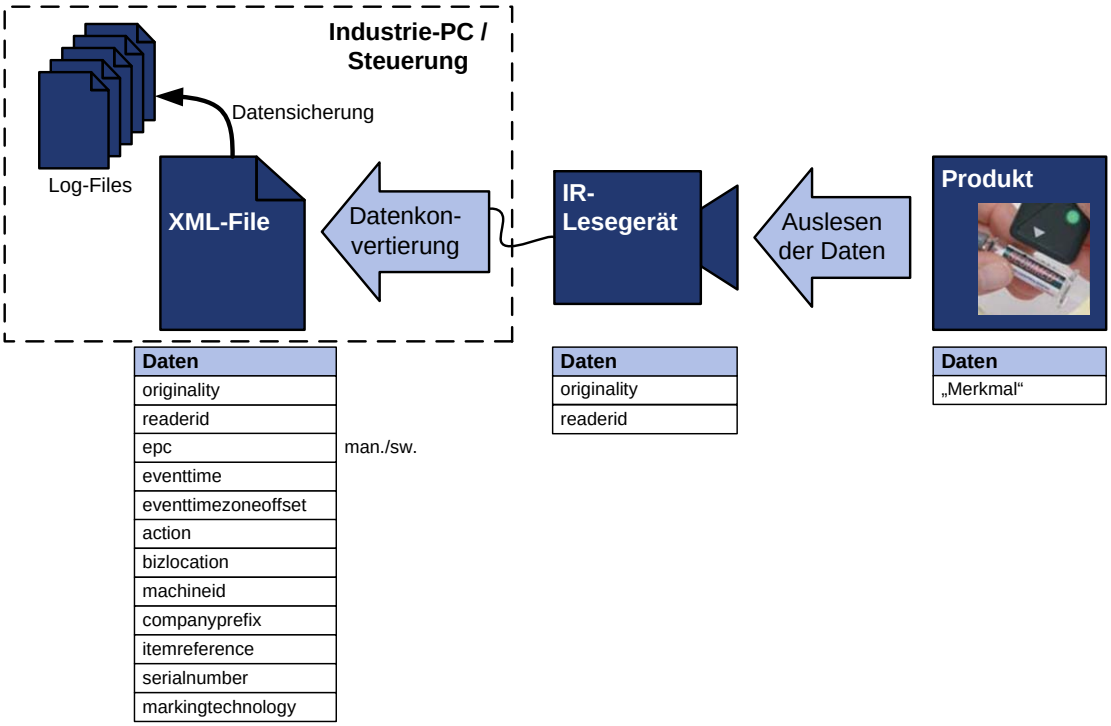


Abbildung 20: IP-Punkt zur Authentifizierung von Produkten, die mit IR-Farben gekennzeichnet sind

Abbildung 21: Realisierung eines IP-Punkt am Demonstrator des Lehrstuhl fml zur Authentifizierung von Produkten, die mit IR-Farbe gekennzeichnet sind

3.4.3.2 Vor- und Nachteile der IR-Farben

Die größten Vorteile liegen darin, dass IR-Farben einfach aufzubringen und preisgünstig sind. Zusätzlich sind diese aufgrund der erstellbaren IR-Farbprofile sehr sicher gegenüber Nachahmung. Da die Farbpartikel für das menschliche Auge un-

sichtbar sind, handelt es sich um eine verdeckte Markierung, die von einem Nachahmer nicht ohne weitere Hilfsmittel entdeckt werden kann.

Nachteilig ist, dass es sich um ein reines Originalitätskennzeichen handelt, das eine Unterscheidbarkeit einzelner Objekte nicht ermöglicht. Ein EPC kann also in das IR-Kennzeichen nicht integriert und muss separat aufgebracht werden. Auch muss für eine Prüfung die Stelle, an der die IR-Farbmarkierung zu finden ist, bekannt sein, da diese für einen prüfenden Mitarbeiter nicht sichtbar ist.

3.4.4 IP-Punkt für Hologramme

An einem IP-Punkt für Hologramme sind die Sicherheitsmerkmale rein visuell zu authentifizieren. Gleichzeitig ist damit aber die Anforderung der lokalen Authentifizierung erfüllt. Um das Prüfergebnis für eine Dokumentation festzuhalten, kann dieses zusammen mit weiteren Prüfdaten manuell an einem Rechner eingegeben und zur weiteren Verarbeitung an eine Software übergeben werden.

3.4.4.1 Datenmodell für Hologramme, Erzeugung und Authentifizierung mittels Hologrammen

Wie bei IR-Farben wird mit Hologrammen lediglich eine Ja-Nein-Aussage als Argument codiert:

- Originalität.

Hologramme sind sehr aufwändig herzustellende 2D- oder 3D-Darstellungen und werden oftmals als Klebe- oder Vergussetiketten am Produkt angebracht.

Zur Authentifizierung prüft ein qualifizierter Mitarbeiter das Hologramm und entscheidet, ob es sich um ein Original handelt (vgl. Abbildung 22). Da weder dieses Prüfergebnis noch weitere Daten automatisiert ausgelesen werden, ist in diesem Fall eine manuelle Eingabe zur Dokumentation der Prüfung denkbar.

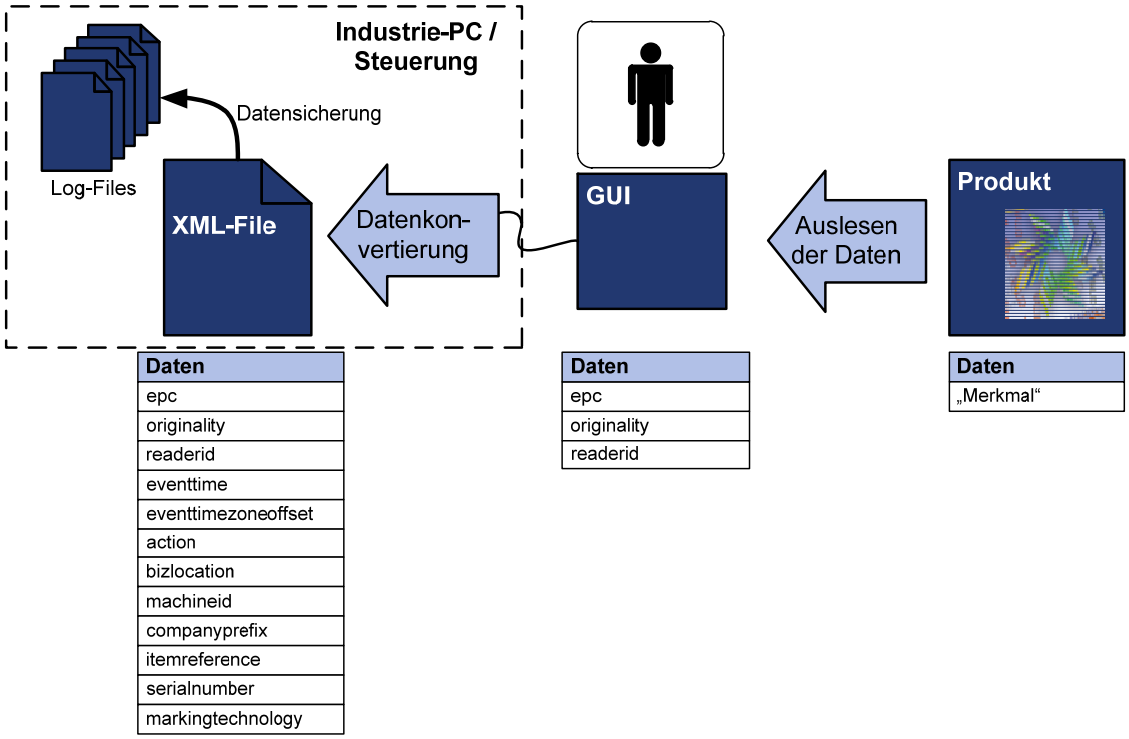


Abbildung 22: IP-Punkt zur Authentifizierung von Produkten, die mit Hologrammen gekennzeichnet sind

Abbildung 23: Realisierung eines IP-Punkts am Demonstrator des Lehrstuhl fml zur Authentifizierung von Produkten, die mit Hologrammen gekennzeichnet sind

3.4.4.2 Vor- und Nachteile von Hologrammen

Bei Hologrammen handelt es sich um offene Sicherheitsmerkmale, die ein Produkt in der Anmutung aufwerten und somit hohe Qualität vermitteln können. Hologramme sind zwar aufwändig in der Herstellung jedoch ab gewissen Stückzahlen sehr preiswerte Sicherheitsmerkmale, die einfach am Produkt an-/eingebracht werden können.

Nachteilig ist, dass Hologramme zwar nicht kopiert, jedoch ähnlich nachgemacht werden können und dann nur noch von qualifizierten Mitarbeitern vom Original zu unterscheiden sind. Außerdem ist es nicht möglich, maschinenlesbar Daten in das Hologramm zu schreiben. Somit kann nur eine manuelle Prüfung und an einem IP-Punkt zur Dokumentation nur eine manuelle Eingabe des Prüfergebnisses erfolgen. Dies stellt grundsätzlich eine Fehlerquelle dar.

3.5 Integration der IP-Punkte in ein IT-Gesamtsystem

3.5.1 Aufbau von IP-Punkten und Struktur der XML-Dateien

Ein IP-Punkt kann prinzipiell alle vier in Abschnitt 3.2 ausgewählten Technologien vereinen (vgl. Abbildung 24, Abbildung 25). Auch können weitere Technologien hinzugefügt werden. Denn aufgrund der Architektur und der Nutzung der XML-Datei als Datenschnittstelle ist das Gesamtsystem offen für weitere Technologien.

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-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. Dabei sind Angaben zu den Fragen wo, was, wann, warum beinhaltet (in Anlehnung an [EPC-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
- Eventtimezoneoffset: Zeitverschiebung gegenüber der weltweit gültigen koordinierten Weltzeit

- Action: Angabe über den Lebenszyklusstatus eines Produktes
- 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 einer Sachnummer
- Markingtechnology: Genutzte Sicherheitstechnologie

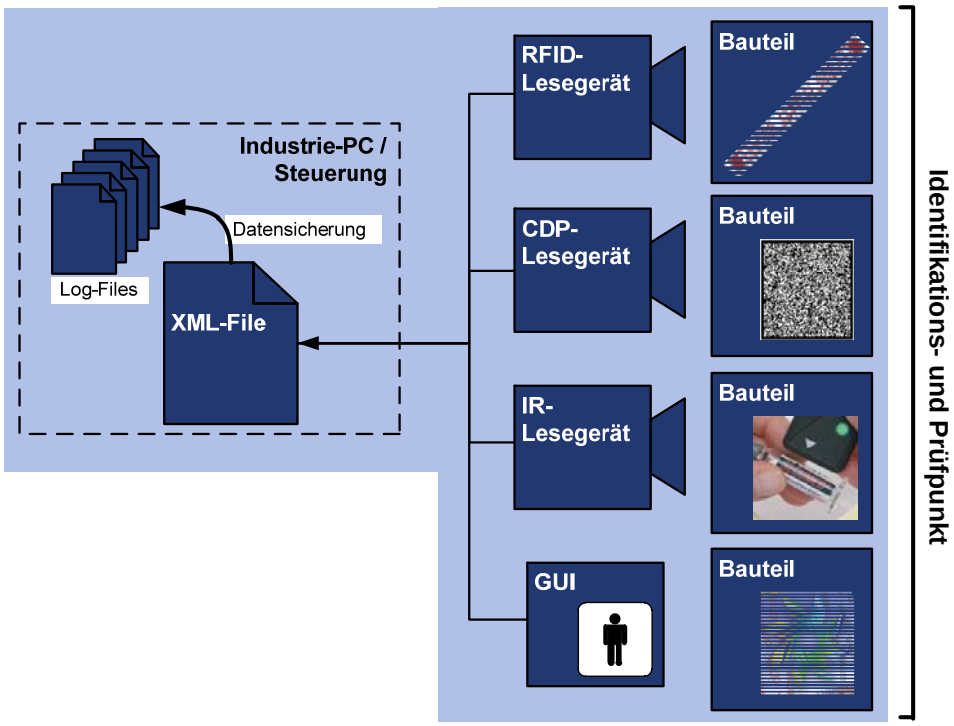


Abbildung 24: Integrierter IP-Punkt für RFID, CDP, IR-Farben und Hologramme

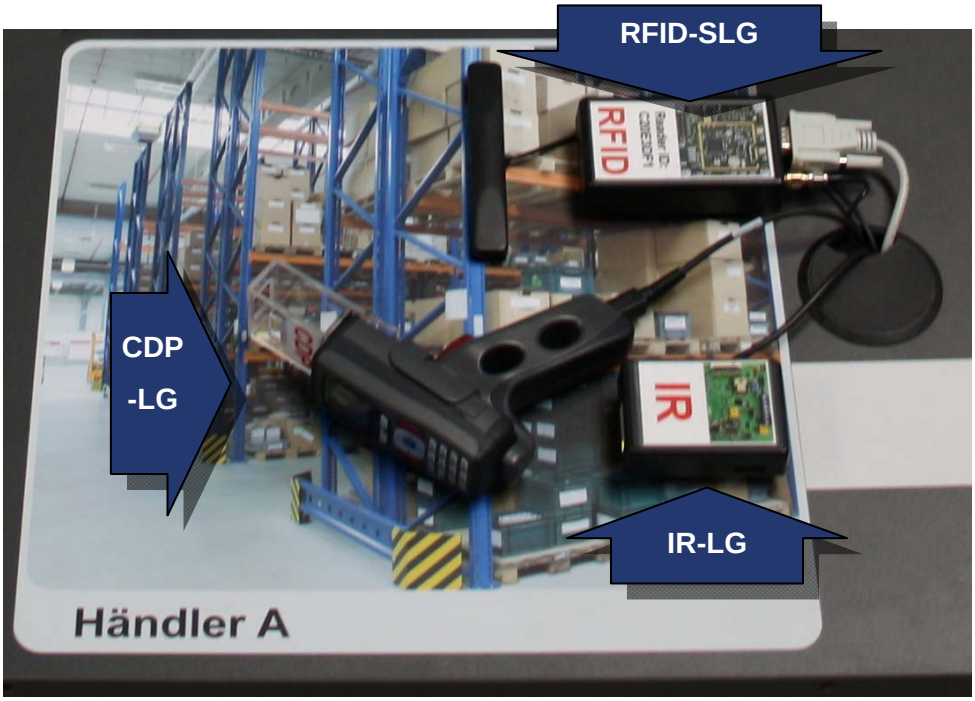


Abbildung 25: Realisierung eines integrierten IP-Punkts für RFID, CDP, IR-Farben und Hologramme am Demonstrator des Lehrstuhl fml (Hologramme werden mittels manueller Eingabe erfasst)

Je Prüfvorgang wird an jedem IP-Punkt eine XML-Datei, auch als „Event“ bezeichnet, erzeugt und hat die in Abbildung 26 abgebildete Form.

```xml
<?xml version="1.0" encoding="utf-8" standalone="yes" ?>
- <epcis:EPCISDocument xsi:schemaLocation="urn:epcglobal:epcis:xsd:1 EPCglobal-
  epcis-1_0.xsd" creationDate="2008-03-16T22:13:16.397+01:00"
  xmlns:epcglobal="urn:epcglobal:xsd:1"
  xmlns:proauthent="http://de.tum.mw.fml.proauthent" schemaVersion="1.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:epcis="urn:epcglobal:epcis:xsd:1">
  - <EPCISBody>
    - <EventList>
      - <ObjectEvent>
          <eventTime>2010-04-22T12:34:42.750+01:00</eventTime>
          <eventTimeZoneOffset>+01:00</eventTimeZoneOffset>
        - <epcList>
            <epc>urn:epc:id:giai:80000001.27777777777277001</epc>
          </epcList>
          <action>OBSERVE</action>
        - <bizLocation>
            <id>Kunde_A</id>
          </bizLocation>
          <proauthent:tid>01331000097D3827</proauthent:tid>
          <proauthent:originality>true</proauthent:originality>
          <proauthent:readerid>D8ED2712</proauthent:readerid>
          <proauthent:companyprefix>P80000001</proauthent:companyprefix>
          <proauthent:itemreference>P27777777777</proauthent:itemreference>
          <proauthent:serialnumber>P277001</proauthent:serialnumber>
          <proauthent:machineid>PMaschine_A1</proauthent:machineid>
          <proauthent:trustservice />
          <proauthent:technology>rfid</proauthent:technology>
        </ObjectEvent>
      </EventList>
    </EPCISBody>
  </epcis:EPCISDocument>
```


Abbildung 26: XML-Datei

Die XML-Dateien werden zur lokalen Sicherung und Nachvollziehbarkeit der Historie nach der Erzeugung auch als Logdatei gespeichert (auch als Protokolldatei bezeichnet, vgl. „Log-Files“ in Abbildung 24). Diese Logdateien können im Bedarfsfall am lokalen System angezeigt und somit historische Events nachvollzogen werden.

3.5.2 Datenübertragung, -hosting und -nutzung

Die je Prüfvorgang an einem IP-Punkt generierten XML-Dateien können in eine zentrale oder auch dezentrale Datenbank zur weiteren Verarbeitung geladen werden. Hierfür bieten sich SQL-Datenbanken an (Structured Query Language, Standardsprache für relationale Datenbanken [Ten-06]). Die Datenübertragung ist mittels einer Online-Verbindung via Internet oder mithilfe eines Wechseldatenträgers möglich (vgl. Abbildung 27).

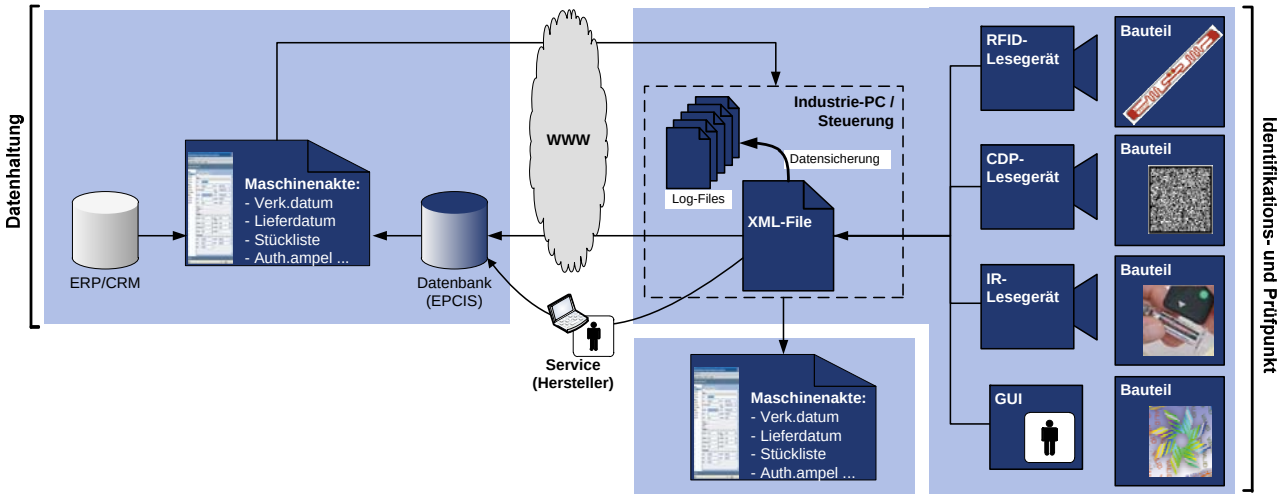


Abbildung 27: IT-Systemarchitektur

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 [EPC-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 (vgl. Abbildung 8), wurde der Report über die Produkte als „Maschinenakte“ ausgestaltet (vgl. Abbildung 27). 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 möglich und gibt somit eine Sicht auf den aktuellen Zustand der ausgewählten Maschine. Die Maschinenakte kann sowohl vom Hersteller der Produkte, vom Maschinenbetreiber oder anderen Beteiligten der Wertschöpfungskette, die einen IP-Punkt betreiben, eingesehen werden.

Zentrales Argument des gesamten Systems ist der EPC, der eine entsprechende Generierung und datentechnische Verknüpfung von Events ermöglicht. Deshalb ist dieses Argument entweder in den Sicherheitsmerkmalen maschinenlesbar codiert

(vgl. RFID und CDP in den Abschnitten 3.4.1.1 und 3.4.2.1) oder muss zur Generierung der Events softwareseitig bzw. manuell ergänzt werden (vgl. IR-Farben und Hologramme in den Abschnitten 3.4.3 und 3.4.4).

3.5.3 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 Piraterieschutz auf die gesamte Wertschöpfungskette ausgeweitet werden.“ ([Wil-07] S.8)

Daher werden im Projekt zum Schutz des gesamten Wertschöpfungsnetzes an allen relevanten Stellen IP-Punkte errichtet (vgl. Abbildung 28, Abbildung 29). 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.

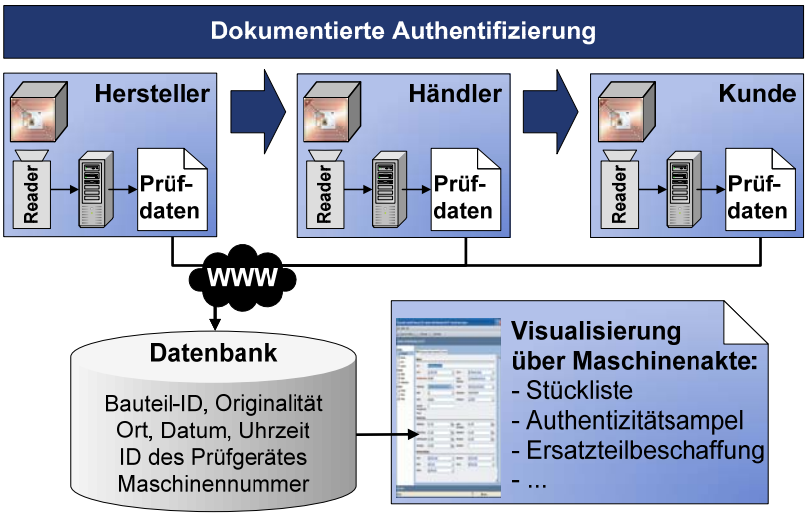


Abbildung 28: IP-Punkte entlang der geschützten Wertschöpfungskette

Abbildung 29: Realisierung einer geschützten Wertschöpfungskette als Demonstratorsystem des Lehrstuhl fml mit drei IP-Punkten

3.6 Realisierung von Zusatznutzen

Um das Gesamtsystem, wie es in den Abschnitten 3.4 bis 3.5 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. Dabei gibt es 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 4 und Tabelle 5 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 4: Lokal an einem Bauteil / einer Maschine zu realisierende Zusatznutzen

Zentral im System		
Ersatzteilmanagemet	**Service**	**Betriebswirtschaft und 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 5: Zentral im System zu realisierende Zusatznutzen

In der Realisierung als Demonstrator am Lehrstuhl fml konnten folgende Zusatznutzen realisiert werden (vgl. Abbildung 29):

- Steigerung der Qualitätsanmutung bzw. Kennzeichen als Gütesiegel
- grünes Leuchtsignal als Information ohne Bestätigungserfordernis durch Maschinenbediener
- Erstellung bzw. Aktualisierung einer tatsächlichen, realen Maschinenstückliste
- Nachverfolgbarkeit der Ersatzteile auf dem Transportweg.

Bei den Anwenderunternehmen wurden in deren Pilotinstallationen mit Unterstützung des Lehrstuhl fml die in Tabelle 6 gelisteten Zusatznutzen umgesetzt.

Homag	Multivac	Vollmer
• Automatische Bauteil-/ Werkzeugidentifikation • Verwechslungsschutz für Bauteile und Werkzeuge • Selbstkonfiguration bei Originalbauteilen • Condition Monitoring *	• Automatische Bauteil-/ Werkzeugidentifikation * • Verwechslungsschutz für Bauteile und Werkzeuge * • Serviceampel * • Condition Monitoring * • Erleichterte Ersatzteilbeschaffung *	• Automatische Bauteil-/ Werkzeugidentifikation • Verwechslungsschutz für Bauteile und Werkzeuge • Automatische Datenübergabe bauteil- oder werkzeugindividueller Parameter • Serviceampel * • bessere Vorbereitung der Servicetechniker *

Tabelle 6: In Pilotinstallationen der Anwenderunternehmen realisierte Zusatznutzen
***) Zur Realisierung vorbereitet**

3.7 Absicherung: Risikoanalyse und Pilotinstallationen

Zur Absicherung des gesamten in ProAuthent enwickelten IT-Systems zur Kennzeichnung und dokumentierten Authentifizierung von schützenswerten Bauteilen wurde dieses einer Schwachstellenanalyse unterzogen. Dabei wurden zwei Ziele verfolgt: einerseits das Aufdecken möglicher Angriffspunkte für Nachahmer, andererseits das Listen von Gegenmaßnahmen, um bei realen Umsetzungen bei Unternehmen die gefundenen Schwachstellen eliminieren zu können.
Dabei wurden 73 Schwachstellen mit verschiedenen Ursachen, somit 105 Einzelfälle gefunden, bewertet und Gegenmaßnahmen formuliert. Darunter entfallen auf die Bereiche:

- RFID: 21 Fälle bei 14 Schwachstellen
- CDP: 20 Fälle bei 13 Schwachstellen
- IR: 22 Fälle bei 15 Schwachstellen
- Hologramm: 16 Fälle bei 12 Schwachstellen
- System allgemein: 26 Fälle bei 19 Schwachstellen

Die Bewertung aller Fälle mit einer Risikoprioritätszahl ermöglichte die Gewichtung der einzelnen Schwachstellen und somit die Wichtigkeit, die jeweiligen Gegenmaßnahmen bei Realisierungen zu berücksichtigen. Die wichtigsten Erkenntnisse sind.

- RFID:
  - Das vorsätzliche Abschirmen eines Transponders oder des SLG ist jederzeit möglich.
  - + Weder die Nachahmung noch die Übertragung des Kennzeichens werden als kritisch eingestuft.
  - + RFID gilt als sehr sicher bzw. als sehr sicher gestaltbar.
- CDP:
  - Sofern die Originalvorlage des CDPs aus interner Nachlässigkeit oder externer Angriffe öffentlich wird, können Kopien als Originale gekennzeichnet werden.
  - Die Verschmutzung des Kennzeichens, der Luftschnittstelle oder des Lesegerätes stellt eine potenzielle Ursache für Störungen dar.
  - + Die Nachahmung des Kennzeichens ist unkritisch, da es mit heutiger Technik nicht kopiert werden kann.
  - + Bei Beherrschung der Schwachstellen ist das CDP eine sehr gute Möglichkeit, ein optisches Unikatkennzeichen zur Verfügung zu haben.
- Infrarotfarben:
  - Die manuelle oder automatische Ergänzung des EPCs zur Erstellung einer XML-Datei könnte fehlerhaft sein.
  - Die Verschmutzung des Kennzeichens, der Luftschnittstelle oder des Lesegerätes stellt eine potenzielle Ursache für Störungen dar.
  - + Die Nachahmung des Kennzeichens wird als unwahrscheinlich eingeschätzt.
- Hologramm:
  - Die manuelle oder automatische Ergänzung des EPCs zur Erstellung einer XML-Datei könnte fehlerhaft sein.
  - Hologramme können zwar nicht kopiert, aber nachgeahmt werden.
- System allgemein:
  - Der Schutz der XML- und Log-Dateien muss auf den lokalen Datenträgern sichergestellt werden, da eine Manipulationsmöglichkeit das Gesamtsystem in Frage stellt.
  - Die Datenübertragungswege von den lokalen IP-Punkten zu den Datenbanken müssen insbesondere bei manueller Datenübertragung abgesichert werden.

- Die Datenübertragungsfrequenz muss ausreichend hoch sein, um die Aktualität der Daten im System zu garantieren.
- Die Datenbanken müssen hinreichend vor unautorisiertem Zugriff von außen geschützt werden.

Die Übertragbarkeit des entwickelten ProAuthent-Systems in reale Anwendungen konnte durch das Errichten von drei Pilotinstallationen bei den Anwenderunternehmen Homag, Multivac und Vollmer nachgewiesen werden. Dabei wurden nach dem Vorbild des theoretisch erarbeiteten und im Demonstrator des Lehrstuhls fml erstmalig realisierten IT-Systems eigene Pilotanwendungen entwickelt und umsetzt. Die Übertragung des Systems auf die jeweilige Pilotmaschine konnte in jedem Fall erfolgreich durchgeführt, die Pilotinstallation konnte jeweils vollständig in Betrieb genommen werden (vgl. Abschnitt 6).

3.8 Juristische Aspekte

Um das Gesamtsystem auch von der juristischen Seite abzusichern, wurde dieses durch den Lehrstuhl für Wirtschaftsrecht und Geistiges Eigentum der Technischen Universität München 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 vereinbart werden, wobei das Wettbewerbsrecht und AGB-Recht berücksichtigt werden muss, vor allem bezüglich der gegenständlichen und zeitlichen Höchstdauer der Bindung.

3.9 Zusammenfassung

Im Forschungsprojekt ProAuthent konnte 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. Somit steht den Unternehmen dieser Branche 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.

4 Planung und Ablauf des Vorhabens

Ende 2008 musste das Projektkonsortium umgebildet werden. Grund dafür war im Oktober 2008 der Austritt der Firma Siempelkamp Maschinen- und Anlagenbau GmbH & Co. KG aus dem Projekt, der durch eine neue strategische Ausrichtung des Unternehmens nach einem Führungswechsel in der Geschäftsleitung begründet wurde. Nach kurzer Suche nach einem adäquaten neuen Projektpartner konnte die Firma Müller Martini GmbH gewonnen werden, welche das budgetäre Engagement bzw. budgetären Anteile der Firma Siempelkamp vollständig und die Arbeitspakete inhaltlich teilweise übernehmen konnte. Gewisse inhaltliche Anpassungen in der spezifischen Vorhabensbeschreibung mussten vorgenommen und in den Gesamtkontext eingegliedert werden. Dies wurde im Antrag vom 26.11.2008 von Müller Martini formuliert und eingereicht und bis Januar 2009 abgeschlossen.
Aufgrund der schweren Wirtschaftskrise ab Ende des Jahres 2008, die ausgelöst war durch die Banken- und Finanzkrise, die im Frühsommer 2007 mit der US-Immobilienkrise begann, waren die beteiligten Anwenderunternehmen Homag Group AG, Multivac Sepp Haggenmüller GmbH & Co. KG, Vollmer Werke Maschinenfabrik GmbH sowie Müller Martini GmbH zu Kurzarbeit gezwungen und konnten die für sie vorgesehenen Arbeitspakete nicht planmäßig ausführen. Auch gab es bei mehreren Projektpartnern während der Gesamtlaufzeit des Projektes aufgrund personeller sowie persönlicher Veränderungen Projektleiterwechsel. Beim Aufbau des Demonstrators sowie der Installation der Pilotanwendungen mussten Verzögerungen aufgrund von Lieferengpässen hingenommen werden. Durch diese Faktoren kam es im Projektverlauf zu Verzögerungen, die sich bis zum Projektende hin aufsummierten und nicht mehr aufholen ließen. Daher wurde für das Teilkonsortium bestehend aus

- Homag Group AG
- Infoman AG
- Lehrstuhl für Fördertechnik Materialfluss Logistik
- Müller Martini GmbH
- Multivac Sepp Haggenmüller GmbH & Co. KG
- Schreiner Group GmbH & Co. KG
- Vollmer Werke Maschinenfabrik GmbH

eine Laufzeitverlängerung um zwei Monate beantragt und durch den Projektträger mit Schreiben des 09.12.2010 bewilligt. Das Projekt endete für die genannten Projektpartner somit am 31.03.2011.

5 Ergebniszusammenfassung

Mit dem System zur Kennzeichnung und Authentifizierung von kritischen Bauteilen im Maschinen- und Anlagenbau ist es erstmals möglich, schützenswerte Bauteile von betroffenen Unternehmen gezielt mit Sicherheitsmerkmalen zu versehen. Das gesamte entwickelte IT-System ermöglicht darauf aufbauend den Schutz des gesamten Wertschöpfungsnetzwerks. Somit wurde ein technischer, präventiv wirkender Schutz vor Produktpiraterie entwickelt (eine ausführliche Darstellung mit Bildern und Tabellen ist in Abschnitt 3 zu finden). Im Forschungsprojekt ProAuthent sind verschiedene Erkenntnisse und wichtige Ergebnisse zentral (vgl. Abschnitt 3):

- Mit einem methodisch unterstützten Vorgehen lassen sich schützenswerte Bauteile von betroffenen Unternehmen und passende Kennzeichnungs- und Authentifizierungstechnologien ermitteln (vgl. Abschnitte 3.1 und 3.2).
- Zur Kennzeichnung von Ersatzteilen und Komponenten können verschiedene Kennzeichnungstechnologien als Orignalitäts- oder Unikatkennzeichen verwendet werden (vgl. Abschnitte 3.2 und **Fehler! Verweisquelle konnte nicht gefunden werden.**).
- 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 3.4).
- Bei RFID können kostengünstige, passive UHF-Transponder zur lokalen Authentifizierung genutzt werden, sofern das im Forschungsprojekt entwickelte kryptografisch Verfahren zur Erzeugung und Entschlüsselung der Signatur verwendet wird (vgl. Abschnitte 3.4.1.2 und 3.4.1.3).
- Das Rauschmuster CDP kann selbst Daten kodieren und kann auf metallene Oberflächen gelasert werden (vgl. Abschnitt 3.4.2.1).
- Zur Dokumentation der Prüfergebnisse können an den IP-Punkten lokal XML-Dateien als „Prüfevent“ erzeugt und in zentral Datenbanken übermittelt werden (vgl. Abschnitt 3.5)
- Dadurch ist zeitgleich der Aufbau eines Tracking-&-Tracing-Systems möglich, welches das gesamte Wertschöpfungsnetzwerk vor Kopien schützen kann (vgl. Abschnitt 3.5.3).

- 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 3.6)
- 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 3.7).
- Das System ist juristisch geprüft und bei entsprechender vertraglicher Regelung vollständig rechtskonform (vgl. Abschnitt 3.8).

6 Nutzen für das Unternehmen, insbesondere Verwertbarkeit des Ergebnisses

Im Forschungsprojekt ProAuthent konnten die Anwenderunternehmen Homag, Multivac und Vollmer nach dem Vorbild des theoretisch erarbeiteten und im Demonstrator des Lehrstuhls fml erstmalig realisierten IT-Systems zur dokumentierten Authentifzierung gekennzeichneter Objekte eigene Pilotinstallationen entwickeln und umsetzen. Die Übertragung des Systems auf die jeweilige Pilotmaschine konnte in jedem Fall erfolgreich durchgeführt und vollständig in Betrieb genommen werden.

Die vorgeschlagene IT-Systemstruktur konnte von allen Anwenderunternehmen in der jeweiligen Pilotinstallation mit den Hauptfunktionen

- Kennzeichen und dessen Aufbringung auf die entsprechenden Bauteile (vgl. Abbildung 14)
- Lesegerät
- Lokale Datenauswertung und Speicherung
- Datenübertragung in die zentrale Datenbank
- Einrichtung und Betrieb einer zentralen Datenbank

umgesetzt werden (vgl. Abbildung 30 und Abbildung 31).

Legende zu Abbildung 30 und Abbildung 31:

- In der Ist-Installation umgesetzt
- In der Ist-Installation nicht umgesetzt
- In der Ist-Installation nicht umgesetzt, da dies nicht genutzt wurde.

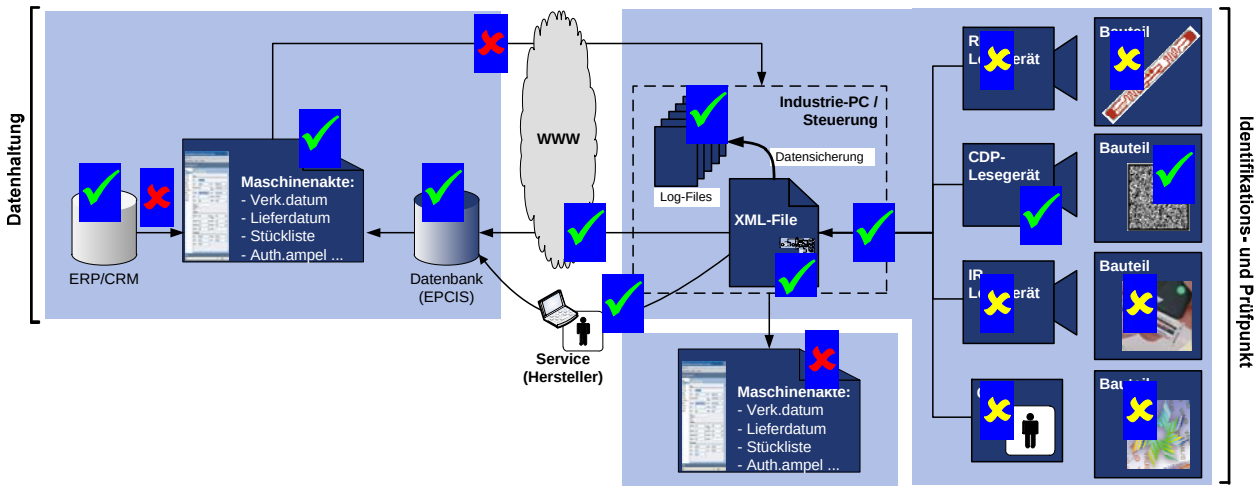


Abbildung 30: Umsetzung der IT-Systemstruktur bei Fa. Homag in der Ist-Installation

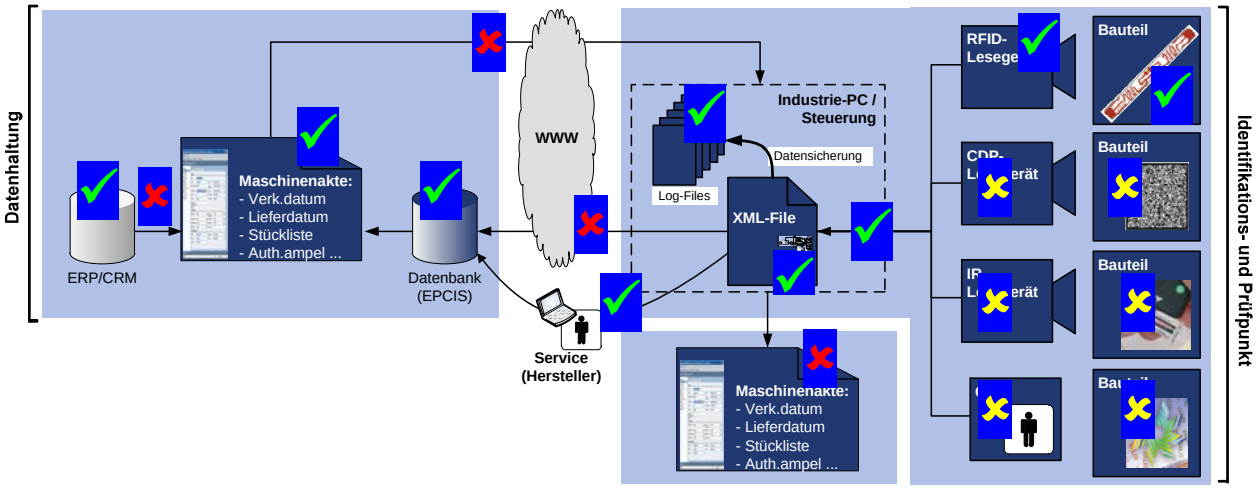


Abbildung 31: Umsetzung der IT-Systemstruktur bei Fa. Multivac und Vollmer in der Ist-Installation

Insgesamt sind zentrale zusammenfassende Aussagen:

- Jedes Anwenderunternehmen hat die ausgewählten schützenswerten Bauteile mit den entsprechenden Unikatkennzeichen markiert.
- In allen Pilotinstallationen kann die Originalität der gekennzeichneten Bauteile mittels der installierten Lesegeräte und Auswerteeinheiten festgestellt werden.
- In jeder Umsetzung werden lokal erzeugte Daten in einer „Schnittstellendatei“ abgelegt, welche gleichzeitig als Log-Datei dient.
- Bei jeder Installation ist eine Datenbank verfügbar.
- Die lokal erzeugten Daten können immer in die eingerichteten Datenbanken übertragen werden.
- Auswertungen auf den Daten sind teilweise (Vollmer, Multivac) bzw. auch vollständig (Homag) möglich.
- Zusatznutzen konnten teilweise realisiert werden.

Durch die Pilotinstallationen bei den Firmen Homag, Multivac, Vollmer konnte die Umsetzbarkeit des Gesamtsystems in industriellen Anwendungen grundsätzlich gezeigt werden und die Unternehmen haben mit der Erstrealisierung umfangreiches Wissen für die weitere Verwertung gesammelt, um ihre Produkte gegen Produktpiraterie zu schützen. Auch können die Unternehmen sicher sein, ein juristisch geprüftes System aufzubauen, das bei entsprechender vertraglicher Regelung vollständig rechtskonform ist (vgl. Abschnitt 3.8). Darüber hinaus können die Anwenderunternehmen durch Nutzung der Auswahlmethodik (vgl. Abschnitte 3.1 und 3.2) weitere schützenswerte Bauteile sowie passende Kennzeichnungstechnologien bestimmen, um die Teile mit Sicherheitsmerkmalen zu versehen.

7 Zusammenarbeit mit anderen Stellen außerhalb des Verbundprojektes

Zur Abstimmung von Projektinhalten sowie Nutzung von Synergien wurde ein Arbeitskreis „Pro-4“ eingerichtet, in dessen Rahmen zu Beginn der Forschungsvorhaben wertvolle Hinweise ausgetauscht und Absprachen getroffen werden konnten. An diesem Arbeitskreis waren neben ProAuthent die Projekte „ProOriginal“, „ProProtect“ und „Protactive“ beteiligt – zeitweise waren in diesem Kreis auch die Projekte „Kopikomp“ sowie „ConImit“ vertreten.

In direktem Austausch mit dem Forschungsprojekt ProProtect wurde die in ProAuthent geplante IT-Systemarchitektur analysiert und auf Schwachstellen hin untersucht.

Auch konnte im Bereich der Kennzeichnungstechnologien ergänzendes Know-how durch den Austausch mit der Firma U-NICA International AG in das Projekt ProAuthent geholt und das Vorgehen im Forschungsprojekt abgesichert werden.

8 Darstellung des bekannt gewordenen Fortschritts bei anderen Stellen

Im Themenfeld „Innovationen gegen Produktpiraterie“ des Rahmenkonzepts „Forschung für die Produktion von morgen“ des Bundesministeriums für Bildung und Forschung arbeiteten insgesamt elf Projekte – neben ProAuthent

- ConImit
- EZ-Pharm
- KoPiKomp
- KoPira
- MobilAuthent
- O-PUR
- PiratPro
- ProOriginal
- Pro-Protect
- PROTACTIVE.

Eine Übersicht über die Projekte gibt die Homepage des Projektes ConImit [Con-11].

In diesen Forschungsprojekten wurden zahlreiche, unterschiedlichste Bereiche des Themenfeldes Produktpiraterie erforscht und Gegenmaßnahmen entwickelt. Die für ProAuthent wichtigsten Inhalte wurden in den folgenden Projekten erarbeitet:

- ProOriginal:
  Authentifizierung intelligenter Komponenten in Maschinen durch Challenge-Response-Verfahren.
- MobilAuthent:
  Lösung bestehend aus den Bausteinen: Produktkennzeichnung, Produktauthentifizierung, Produktverfolgung, Verwalten und Bereitstellen produktindividueller Daten; dabei Einsatz von RFID zur Kennzeichnung der Produkte.
- EZ-Pharm:
  Elektronisch gesicherte Verpackung mit druckbaren UHF-Transponderantennen, darauf basierend die geschützte Prozesskette von der Produktion der Medikamente bis zum Patienten.

9 Veröffentlichungen, Vorträge, Referate, etc.

In den folgenden Tabellen sind abgebildet

- Veröffentlichungen
- Vorträge
- Messeauftritte

aller am Verbundprojekt beteiligten Partner. Die Beiträge des Lehrstuhl fml sind schwarz, die Beiträge weiterer Projektpartner in grau abgedruckt.

Legende:

Text	Beiträge des Lehrstuhl fml
Text	Beiträge weiterer Projektpartner

Veröffentlichungen				
Titel	**Veröffentlicht in**	**Datum**	**Autor**	**Projektpartner**
Wenn sich Maschine und Komponente kennen	Intelligenter Produzieren	06/2007	Doll, U.,	Homag AG
Gemeinsam gegen Produktpiraterie	PackReport	04/2008	o.V.	Schreiner ProSecure
BMBF Research Project Develops Innovative Protection Solutions	Product&Image Security	06/2008	o.V.	Schreiner ProSecure
Innovative Schutzlösungen	Technik + Einkauf	06/2008	o.V.	Schreiner ProSecure
University Partnership to fight piracy	www.prosecurityzone.com	16.06.08	Schreiner Group	Schreiner ProSecure
Forschungsprojekt gegen Produktpiraterie	www.security-insight.de	26.03.08	o.V.	Schreiner ProSecure
BMBF-Forschungsprojekt entwickelt innovative Schutzlösungen	www.visavis.de	20.03.08	o.V.	Schreiner ProSecure
Joining Forces to combat product piracy	Schreiner Forum Spring 2008 (Englisch+Deutsch)	03/2008	o.V.	Schreiner ProSecure
Produktpiraten – bald ohne Enterhaken?	Faszination Forschung 3 / 08	10/2008	Gudrun Kosche	TUM-Lehrstühle der TU München (BWL, fml, Wirtschaftsrecht)
Methoden und Strategien gegen Produktpiraterie	Industrie Management 6/2008	12/2008	Wildemann, H.	Lehrstuhl BWL, TU München
Herausforderung Produktpiraterie	Industrie Management 6/2008	12/2008	Ann, C., Grüneis, B.	Lehrstuhl Wirtschaftsrecht, TU München
Potenziale des Produktpiraterieschutzes durch kognitive Authentifizierung	Industrie Management 6/2008	12/2008	Günthner, W., Durchholz, J., Meißner, S., Stockenberger, D.	Lehrstuhl fml, TU München

Schutz vor Produktpiraterie im Maschinen- und Anlagenbau	Ideen zünden TV: http://www.hightech-strategie.de/de/1256.php	07/2009	Günthner, W.	Lehrstuhl fml, TU München
Schutz vor Produktpiraterie im Maschinen- und Anlagenbau	Von der Idee zum Produkt - Erfolge der Projektförderung II	07/2009	o.V.	BMBF (Hrsg.)
Kritische Bauteile vor Nachbau schützen	intelligenter produzieren	12/2009	Günthner, W., Durchholz, J., Stockenberger, D.	Lehrstuhl fml, TU München
Das Merkmal macht den Unterschied	Security insight	02/2010	Günthner, W.; Stockenberger, D.	Lehrstuhl fml, TU München
ProAuthent – Integrierter Produktpiraterieschutz durch Kennzeichnung und Authentifizierung von kritischen Bauteilen im Maschinen- und Anlagenbau	ConImit Pressemappe	05.03.10	o.V.	Lehrstuhl fml, TU München
Integrierter Produktpiraterieschutz durch Kennzeichnung und Authentifizierung von kritischen Bauteilen im Maschinen- und Anlagenbau (ProAuthent)	BMBF – Fördermaßnahme „Innovationen gegen Produktpiraterie“	11.03.10	o.V.	Lehrstuhl fml, TU München
Schutz vor Produktpiraterie: Fälschungssichere Kennzeichnung von Bauteilen im Maschinen- und Anlagenbau	Schreiner Group GmbH & Co. KG www.schreiner-group.de	17.03.10	o.V.	Schreiner ProSecure
Fälschungssichere Kennzeichnung von Bauteilen im Maschinen- und Anlagenbau	materialsgate - competence in materials www.materialsgate.de	19.03.10	o.V.	Schreiner ProSecure
Schutz vor Produktpiraterie	Schleißheimer Zeitung Online www.schleissheimer-zeitung.de	20.03.10	o.V.	Schreiner ProSecure
Produktpiraterie: Ersatzteile fälschungssicher kennzeichnen	CAD-Relations Online	24.03.10	o.V.	Schreiner ProSecure
Produktpiraterie: Ersatzteile fälschungssicher kennzeichnen	Konstruktionspraxis Online www.konstruktionspraxis. vogel.de	24.03.10	Juliana Schulze	Schreiner ProSecure
Flagge hissen gegen Produktpiraten – Mit High Tech gegen Technologieklau	www.vdma-webbox.tv	07.04.10	VDMA	VDMA
Protection from Product Piracy – Fake-proof labelling of components in machine and installation construction	Messe Daily Offizielle Messezeitung der Hannover Messe	21.04.10	o.V.	Schreiner ProSecure

Schutz vor Produktpiraterie - Fälschungssichere Kennzeichnung von Bauteilen im Maschinen- und Anlagenbau	Messe Daily Offizielle Messezeitung der Hannover Messe	23.04.10	o.V.	Schreiner ProSecure
Protection from Product Piracy – Fake-proof labelling of components in machine and installation construction	Messe Daily Offizielle Messezeitung der Hannover Messe	23.04.10	o.V.	Schreiner ProSecure
ProAuthent - Wirksamer Schutz vor Produktpiraterie für Komponenten im Maschinen- und Anlagenbau	LIZ Online Newsletter	27.04.10	Durchholz, J.	Lehrstuhl fml, TU München
Documented authentication as an effective protection against coun-terfeiting for components in mechanical engineering	RFID-SysTech 2010	16.06.10	Durchholz, J.; Stockenberger, D.; Günthner, W.	Lehrstuhl fml, TU München
ProAuthent – Integrated Protection against Counterfeiting in Mechanical Engineering through Marking and Authenticating Critical Components	15th ELA Doctorate Workshop 2010	17.06.10	Stockenberger, D.	Lehrstuhl fml, TU München
Lösungen gegen Fälschung im Verbundprojekt Proauthent	Industrieanzeiger 2010/27 (www.industrieanzeiger.de)	05.07.10	o.V.	Schreiner ProSecure
Schreiner ProSecure präsentiert beim Industriearbeitskreis ProAuthent	BlauerBote Online	12.08.10	o.V.	Schreiner ProSecure
Schreiner ProSecure präsentiert beim Industriearbeitskreis ProAuthent Systemlösungen zum Fälschungsschutz von Bauteilen und Anlagen	Schreiner Group GmbH & Co. KG www.schreiner-group.de	12.08.10	o.V.	Schreiner ProSecure
Gemeinsam gegen Plagiate	rfid ready Online www.rfid-ready.de	12.08.10	o.V.	Schreiner ProSecure
Schreiner ProSecure präsentiert beim Industriearbeitskreis ProAuthent Systemlösungen zum Fälschungsschutz von Bauteilen und Anla	Smartmag Online	12.08.10	o.V.	Schreiner ProSecure
Schreiner ProSecure präsentiert beim Industriearbeitskreis ProAuthent Systemlösungen zum Fälschungsschutz von Bauteilen und Anla	materialsgate - competence in materials www.materialsgate.de	13.08.10	o.V.	Schreiner ProSecure
Proauthent: Veranstaltung zeigt Lösungen gegen Produktpiraterie	Sicherheit.Info www.sicherheit.info	13.08.10	o.V.	Schreiner ProSecure

ProAuthent Systemlösungen zum Fälschungsschutz von Bauteilen und Anlagen	Industriepraxis Online	27.08.10	o.V.	Schreiner ProSecure
Piraterieschutz durch Kennzeichnung und Authentifizierung	ConImit-Newsletter Ausgabe 3/2010	30.08.10	o.V.	Lehrstuhl fml, TU München
ProAuthent- Integrierter Produktpiraterieschutz	LIZ Online Newsletter	02.09.10	Durchholz, J.	Lehrstuhl fml, TU München
Fälschungssichere Kennzeichnung von Bauteilen im Maschinen- und Anlagenbau	Bayernmetall	15.09.10	o.V.	Schreiner ProSecure
Dokumentierte Authentifizierung als wirksamer Schutz vor Produktpiraterie für Komponenten im Maschinen- und Anlagenbau	6. Fachkolloquium der Wissenschaftlichen Gesellschaft für Technik und Logistik (WGTL)	29.09.10	Durchholz, J.; Stockenberger, D.; Günthner, W.	Lehrstuhl fml, TU München
„Leitfaden zum Schutz vor Produktpiraterie durch Bauteilkennzeichnung“ veröffentlicht	LIZ Online Newsletter	25.10.10	Durchholz, J.	Lehrstuhl fml, TU München
Proaktiver Schutz vor Piraterie durch Kennzeichnung und Authentifizierung von kritischen Bauteilen im Maschinen- und Anlagenbau	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, Frankfurt am Main 2010	11/2010	Ann, C.; Bender, J.; Doll, U.; Durchholz, J.; Görtz, M.; Günthner, W.; Hauck, R.; Kurz, G.; Miller, W.; Pommer, P.; Schlaucher, W.; Schmidt-Riediger, B.; Schnapauff, K.; Stockenberger, D.; Tschöke, T.; Wildemann, H.	Lehrstuhl BWL, TU München; Lehrstuhl fml, TU München; Lehrstuhl Wirtschaftsrecht, TU München; Homag Holzbearbeitungssysteme GmbH; Infoman AG; Müller Martini GmbH; Multivac Sepp Haggenmueller GmbH & Co.KG; Schreiner Group GmbH & Co. KG; Vollmer Werke Maschinenfabrik GmbH
Leitfaden zum Schutz vor Produktpiraterie durch Bauteilkennzeichnung	-	11.11.10	Durchholz, J.; Günthner; W.; Pommer, P.; Stockenberger, D.; Tschöke, T.; Völcker, T.; Wildemann, H.	Lehrstuhl BWL, TU München; Lehrstuhl fml, TU München; Schreiner Group GmbH & Co. KG
ProAuthent – Integrierter Produktpiraterieschutz durch Kennzeichnung und Authentifizierung von kritischen Bauteilen im Maschinen- und Anlagenbau	Innovationen gegen Produktpiraterie Produktschutz kompakt	16.11.10	o.V.	Lehrstuhl fml, TU München
Fälschungssichere Fingerabdrücke	FM Das Logistikmagazin	12/2010	Gerd Fahry	Schreiner ProSecure

Dokumentierte Authentifizierung als Produktpiraterieschutz – Integrierter Produktpiraterieschutz durch Kennzeichnung von kritischen Bauteilen im Maschinen- und Anlagenbau	RFID im Blick – Sonderausgabe „RFID in der Region München“	02/2011	Stockenberger, D.	Lehrstuhl fml, TU München
Schutz von Produkten im Maschinen- und Anlagenbau durch den Einsatz von RFID	Freimuth, J.; Krieg, R.; Luo, M.; Müller, C.; Schädler, M: Geistiges Eigentum in China – Neuere Entwicklungen und praktische Ansätze für den Schutz und Austausch von Wissen. Gabler, Wiesbaden 2011	03/2011	Günthner, W. A.	Lehrstuhl fml, TU München
Protection against piracy in machine and plant construction	From the Idea to the Product - Project funding successes II	03/2011	o.V.	BMBF (Hrsg.)
Leitfaden zum Schutz vor Produktpiraterie durch Vertragsgestaltung	-	08.03.11	Ann, C.; Günthner, W.; Hauck, R.; Durchholz, J.;Stockenberger, D.	Lehrstuhl fml, TU München; Lehrstuhl Wirtschaftsrecht, TU München
Kennzeichnungstechnologien	Abele, E.; Kuske, P.; Lang, H.: Schutz vor Produktpiraterie. Ein Handbuch für den Maschinenund Anlagenbau. Springer, Berlin, 2011	04/2011	Günthner, W.; Durchholz, J.; Stockenberger, D.	Lehrstuhl fml, TU München
ProAuthent - Wirksamer Schutz vor Produktpiraterie für Komponenten im Maschinen- und Anlagenbau	LIZ Online Newsletter	03.05.11	Stockenberger, D.	Lehrstuhl fml, TU München

Tabelle 7: Veröffentlichungen aller Projektpartner im Rahmen des Forschungsprojektes

Vorträge				
Titel	**Veranstaltung**	**Datum**	**Referent**	**Projektpartner**
ProAuthent – Integrierter Produktpiraterieschutz durch Kennzeichnung und Authentifizierung von kritischen Bauteilen im Maschinen- und Anlagenbau	Innovationen gegen Produktpiraterie, Berlin	22.01.2008	Doll, U.	Homag AG
Integrierter Produktpiraterieschutz für Ersatzteile und Komponenten im Maschinen- und Anlagenbau	3.EUROFORUM-Jahrestagung "Ersatzteilmanagement", Frankfurt/Main	10.09.2008	Doll, U.	Homag AG

ProAuthent - Komponenten und Ersatzteile durch Kennzeichnung und Authentifizierung gegen Produktpiraterie schützen	VDMA ERFA Know-How Schutz, Gera	29.04.2009	Doll, U.	Homag AG
Sichere Authentifizierung von Produkten und deren Verfolgung in der Supply Chain	Presse-Workshop der LOG Logistik-Systembetreuungs-Gesellschaft mbH zu dem Thema „Supply Chain und Produktpiraterie – Innovation im Bereich fälschungssichere Kennzeichnung und mobile Authentifizierung von Produkten“	05.11.2009	Stockenberger, D.	Lehrstuhl fml, TU München
Vermeidung von Komponenten- und Ersatzteilpiraterie durch durchgängige Identifikations- und Authentifizierungstechnologien	DPMA-Konferenz "Durchsetzung von geistigen Eigentumsrechten", Stuttgart	09.11.2009	Doll, U.	Homag AG
Integrierter Produktpiraterieschutz durch Kennzeichnung und Authentifizierung von kritischen Bauteilen im Maschinen- und Anlagenbau	Karlsruher Arbeitsgespräche Produktionsforschung, Karlsruhe	09.03.2010	Doll, U.	Homag AG
ProAuthent - Schutz gegen Produktpiraterie bei Ersatzteilen und Komponenten	VDMA ERFA Produktpiraterie, Denkendorf	27.05.2010	Doll, U.	Homag AG
Documented authentication as an effective protection against coun-terfeiting for components in mechanical engineering	RFID-SysTech 2010	16.06.2010	Durchholz, J.; Stockenberger, D.; Günthner, W.	Lehrstuhl fml, TU München
ProAuthent – Integrated Protection against Counterfeiting in Mechanical Engineering through Marking and Authenticating Critical Components	15th ELA Doctorate Workshop 2010	17.06.2010	Stockenberger, D.	Lehrstuhl fml, TU München

ProAuthent – Integrierter Produktpiraterieschutz durch Kennzeichnung und Authentifizierung von kritischen Bauteilen im Maschinen- und Anlagenbau	Industriearbeitskreis des Forschungsprojektes ProAuthent	21.09.2010	Bender, J.; Doll, U.; Durchholz, J.; Görtz, M.; Hauck, R.; Kurz, G.; Pommer, P.; Schlaucher, W.; Stockenberger, D.; Völcker, T.	Lehrstuhl BWL, TU München; Lehrstuhl fml, TU München; Lehrstuhl Wirtschaftsrecht, TU München; Homag Holzbearbeitungssysteme GmbH; Infoman AG; Müller Martini GmbH; Multivac Sepp Haggenmueller GmbH & Co.KG; Schreiner Group GmbH & Co. KG; Vollmer Werke Maschinenfabrik GmbH
ProAuthent – Demonstration „Schutz gegen Produktpiraterie bei Ersatzteilen und Komponenten“	15. Fachtagung Schüttgutfördertechnik 2010	07.10.2010	Durchholz, J.	Lehrstuhl fml, TU München
RFID-gestützte Datenflüsse in der Supply Chain: ProAuthent – Integrierter Produktpiraterieschutz durch Kennzeichnung und Authentifizierung von kritischen Bauteilen im Maschinen- und Anlagenbau	RFID-Anwendertag	12.10.2010	Stockenberger, D.	Lehrstuhl fml, TU München
ProAuthent – Demonstration „Schutz gegen Produktpiraterie bei Ersatzteilen und Komponenten“	Logistikseminar 2009: Erschließung von Produktivitätspotenzialen in der Logistik	14.10.2010	Stockenberger, D.	Lehrstuhl fml, TU München
ProAuthent Dokumentierte Authentifizierung kritischer Bauteile im Maschinen- und Anlagenbau	Forum:„Den Produktpiraten auf der Spur – Erkennen, Verfolgen, Vorbeugen	19.10.2010	Stockenberger, D.	Lehrstuhl fml, TU München
Schutz vor Know-how Verlust und Produktpiraterie	Maschinenbauforum, Pforzheim	10.11.2010	Doll, U.	Homag AG
Produktpiraterieschutz durch Kennzeichnung und Authentifizierung von kritischen Bauteilen im Maschinen- und Anlagenbau (ProAuthent)	Abschlussveranstaltung „Innovationen gegen Produktpiraterie“	16.11.2010	Völcker, T.	Schreiner ProSecure
Systematische Intensivierung der Kundenbindung zur Prävention vor Produktpiraterie	Kick-Off-Veranstaltung des Kompetenzzentrums gegen Produktpiraterie an der TU Darmstadt	24.02.2011	Bender, J.	Müller Martini GmbH

Tabelle 8: Vorträge aller Projektpartner im Rahmen des Forschungsprojektes

Messeteilnahmen		
Titel	**Datum**	**Projektpartner**
Auftaktveranstaltung, Berlin	13.09.07	Alle Projektpartner des Verbundprojektes ProAuthent
Karlsruher Arbeitsgespräche	09. – 10.03.10	Alle Projektpartner des Verbundprojektes ProAuthent
Hannovermesse 2010	19. – 23.04.10	Alle Projektpartner des Verbundprojektes ProAuthent
Abschlussveranstaltung "Innovationen gegen Produktpiraterie", Berlin	16.11.10	Alle Projektpartner des Verbundprojektes ProAuthent

Tabelle 9: Messeteilnahmen im Rahmen des Forschungsprojektes

10 Abkürzungsverzeichnis

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

11 Abbildungsverzeichnis

12 Tabellenverzeichnis

13 Literaturverzeichnis

[Abe-11] Abele, E.; Kuske, P.; Lang, H.: Schutz vor Produktpiraterie. Ein Handbuch für den Maschinen- und Anlagenbau. Springer, Berlin, 2011

[Ali-10] Alien Technology Corporation: ALN-9640 Squiggle® Inlay. Product Overview. Alien Technology Corporation, Morgan Hill, 2010

[Bar-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

[Bun-05] Bundesministerium des Inneren: Weiterentwicklung der Fälschungssicherheit von Pässen und Personalausweisen. Bundesdruckerein GmbH, Berlin, 2005

[Bun-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

[Chi-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

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

[Con-11] ConImit: Verbundprojekte der Forschungsoffensive "Innovationen gegen Produktpiraterie“. http://www.conimit.de/index.php?id=verbundprojekte Letzter Aufruf: 26.04.2011

[Dur-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

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

[EPC-07] EPCglobal: EPC Information Services (EPCIS) Version 1.0.1 Specification. EPCglobal, Brüssel 2007

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

[Fin-06] Finkenzeller, K.: RFID Handbuch. Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten. Hanser, München, 2006

[FML-11a] Lehrstuhl fml: RFID in der Logistik – Werkzeuge zur Identifikation und Nutzung von RFID Potenzialen. http://www.fml.mw.tum.de/fml/index.php?Set_ID=116. Letzter Aufruf: 12.04.2011

[FML-11b] Lehrstuhl fml: Transparenter Prototyp. http://www.fml.mw.tum.de/fml/index.php?Set_ID=281. Letzter Aufruf: 12.04.2011

[FML-11c] Lehrstuhl fml: RFID-Einsatz in der Baubranche. http://www.fml.mw.tum.de/fml/index.php?Set_ID=261. Letzter Aufruf: 12.04.2011

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

[Hal-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

[Mal-05] Malik, H.; Schindler, S.: Fälschungssichere Verpackungen. Sicherheitstechnologien und Produktschutz. Hüthig, Heidelberg, 2005

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

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

[Nok-09] Nokia Corporation: Nokia 1616 Bedienungsanleitung. http://nds1.nokia.com/ phones/ files/guides/Nokia_1616_UG_de.pdf. Nokia GmbH, Bochum, 2009
Letzter Aufruf: 14.04.2011

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

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

[Sim-11] 3S Simons Security Systems GmbH: ttp://www.3sgmbh.com/referenzen.htm.
Letzter Aufruf: 14.04.2011

[Ten-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

[Völ-06] Völcker, T.: Einsatz innovativer Sicherheitstechnologien für den effektiven Produkt- und Markenschutz. ttp://www.muenchen.ihk.de/mike/ihk_geschaeftsfelder/recht/Anhaenge/Vortrag-Schutz-mit-Sicherheitstechnologie.pdf.
Letzter Aufruf: 14.04.2011

[Vor-09] Vorbrüggen, J.: Schreiner Group GmbH & Co. KG, Bruckmannring 22, 85764 Oberschleißheim, Auskunft am 19.08.2009

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

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

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

[Win-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