Documented authentication as an effective protection against counterfeiting for components in mechanical engineering

Dipl.-Ing. Janina Durchholz, Technische Universität München, Germany, durchholz@fml.mw.tum.de
Dipl.-Wi.-Ing. Dominik Stockenberger, Technische Universität München, Germany, stockenberger@fml.mw.tum.de
Prof. Dr. Willibald A. Günthner, Technische Universität München, Germany, guenthner@fml.mw.tum.de

1 Introduction

Germany's mechanical engineering companies are well-known and globally appreciated for the high quality and functionality of their products. On one hand, this reputation offers itself as a basis for economic success, but on the other hand attracts copyists and counterfeiters, who will readily accept to profit from this development effort by selling counterfeit components and spare parts. For this reason, beside legal und organizational measures there is also a need for technical concepts for anticounterfeiting. [Wil-07] [VDM-08]

Thus six companies and the Technische Universität München have decided to fight product piracy together and develop an effective protection system.

Essentially two approaches for discovering imitations and fakes and thus fighting product piracy exist in today's logistics and trademark protection: The first approach is the application of tracking and tracing functions, which are based on databases which store information about the serialized product's progress through the logistics chain.

The second possibility aims at marking original components with fraud resistant features and the manual control on location. [Rei-08]

Both approaches are reasonable, but also insufficient in certain situations. In the field of mechanical engineering, where mainly components and spare parts are affected, these deficiencies are especially grave. On one hand it is not possible to implement an area-wide online data comparison while on the other hand it is not effective to have information about the components' genuineness available solely on location, as would be possible with conventional measures for trademark protection.

Thus appears the following research question: How can both described approaches be optimally integrated into an efficient protection system against product piracy that fulfills the requirements of mechanical engineering? This question is to be answered in the research project ProAuthent funded by The Federal Ministry of Education and Research (Bundesministerium für Bildung und Forschung, BMBF).

2 Methodology– Approach

The present article initially examines the determined basic functions of an integrated protection system, the specific requirements of the industry mechanical engineering and the essential system components. The decisive demands are especially those which are not adequately addressed by the initially mentioned approaches. This is for example the secure and on-location proof of a product's genuineness through dealers or customers and the simultaneous increase in transparency along the logistics supply chain in order to find weak points and to allow a (re-)traceability of products.

An effective protection system against counterfeiting covers

- menaced components
- with fraud resistant features,
- the ability to check the genuineness feature during the life-time of the product,
- the continuous documentation of all checks and
- the data analysis.

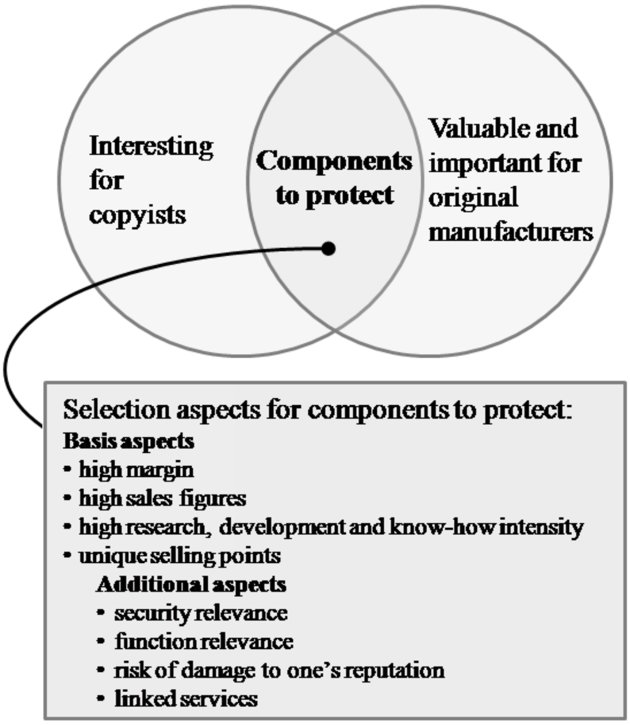
For each of these five sub domains it is necessary to develop secure and applicable solutions which technically and economically fit with the requirements. The complete system will then include a secure marking feature on the component, which is verified at defined identification and authentication points in the supply chain and at last inside the machine. Every check generates a data set or event which is stored in a central database. By this means a data analysis offers comprehensive information about the state of specific machines and components all over the supply chain.

2.1 Menaced components

Marking single products and the later checking always comes with additional expenses. Therefore it is not purposeful to add security marks to each component. It is necessary to identify elements, which are menaced by counterfeiting and also of special interest to the original manufacturer (picture 1). Studying the motivation of falsifiers and comparing this to the manufacturer companies' priorities, specific aspects can be determined as relevant criteria for selecting the components requiring protection. These are products with a high margin, high sales figures, high research, development and know-how intensity and successful products with unique selling points. Additionally security relevance, function relevance, risk of damage to one's reputation and linked services can be regarded.

2.2 Fraud proof marks

For marking critical components, secure marking technologies are necessary. Various types of these are offered by a multitude of companies on the market. For an objective selection of proper technologies a characterization of the multifaceted possibilities for marking a component is indispensable. Marking technologies show important differences in their ability to identify, their life-time and robust-



Picture 1 Aspects for the selection of components to pro tect (Basis and additional aspects)

ness, the limitations and possibilities of the test procedure and the safety. With the help of these parameters it is now possible to structure the existing marking technologies and to develop a methodology which allows a well-grounded selection for concrete scenarios.

The components requiring protection were classified on the same basis. During the analysis of a multitude of mechanical engineering components with respect to the mentioned parameters it becomes evident that typical requirements for the marking technology are existing and the amount of security features can be constrained with respect to their practicability in mechanical engineering.

2.3 Marked components

On the basis of the mentioned parameters, twenty-two marking technologies can be identified as generally possible options. In order to allow one to select one feasible marking approach without having extensive knowledge of this field and without requiring further research, a methodology was developed which permits one to determine a first selection of security marks which should be further proved in the detailed project planning, on the basis of only five variables. The five criteria for this initial choice are:

- the information that is stored inside the marking feature,
- the accessibility at the moment of the inspection,
- the acceptable complexity and cost for checking,
- the required automation level of the checking procedure and
- the available infrastructure.

In the second step leading to the selection of one concrete security feature, further points must be observed. Beside determining the marking position and the mode of attaching the mark to the product, the component's exposure and thus the mechanical stress must be identified as these also influence the marking method. Especially in mechanical engineering requirements are often challenging because the components must be identified not only on their way to the customer but also while built into a machine. At this point the components are often subject to mechanical and chemical influences (e.g. lubricants, friction, vibrations), which make a high robustness of the mark and the bonding between mark and product necessary. These requirements are rare in conventional areas, where such security marks are usually employed. Additional aspects like reading distance at the planned check processes, attainable system security etc. must be considered adequately during the design of the other system components as well.

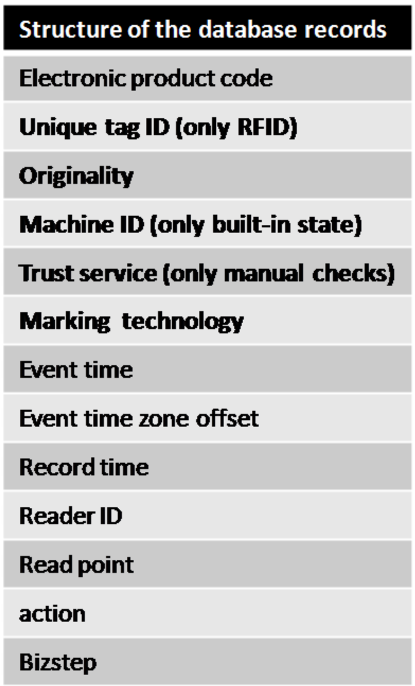
2.4 IT-supported documentation of the checking results

In order to achieve an effective protection against counterfeiting, on top of marking the components requiring protection there is also a need for an IT-supported documentation of the checking results and an analysis of the stored information. Starting from a widespread requirements analysis a detailed concept for fulfilling the following functions was developed: automatic and manual verification of the authenticity on location, central documentation in a database (EPCIS standard [EPCIS-07]) and a well-systematic access to the information, which enables a well-defined response to detected piracy cases.

Verifying components' genuineness is especially important at the time of their installation into the machine or in the built-in state. The customer must be sure not to mistakenly use a fake component no later than this. The original manufacturer also has a legitimate interest in knowing whether original components are installed in the machine for which he supplies service and warranty.

To check the authenticity of components comfortably and securely this should be possible in an automatic and semiautomatic manner. Especially low priced components must also be accessible through a manual process. Thus the IT system comes with interfaces for connecting the readers and also features a user interface for entering the results of manual checking. Hereby the quality of manually created results surely depends on the qualification of the controlling person.

To make the anticounterfeiting system sustainable and versatile, the complete system is consequently built in a modular way. Readers for different marking technologies can be addressed via a standardized format for verification data which can be uniformly handled by the complete system. The developed data format is based on the EPC standard of GS1 [EPCIS-07] [EPC-08] and is thus optimally integrated into existing systems primarily targeting traceability. To store all information necessary for protecting components from counterfeiting, five further entries were added to the obligatory entries of the EPC standard format. Besides stating the genuineness, these contain details about the reader, the controller etc (picture 2).



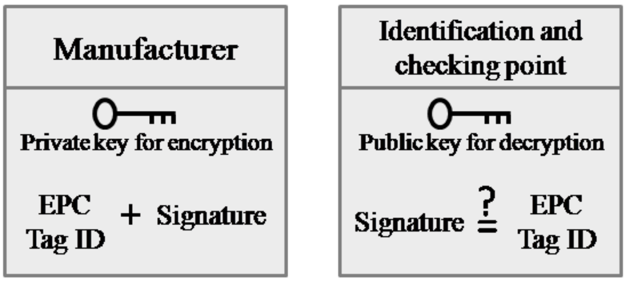
Structure of the database records
Electronic product code
Unique tag ID (only RFID)
Originality
Machine ID (only built-in state)
Trust service (only manual checks)
Marking technology
Event time
Event time zone offset
Record time
Reader ID
Read point
action
Bizstep

Picture 2 Structure of the data sets

Exemplarily the following four marking technologies will be realized in the system: copy detection pattern, IR color pigments, hologram and passive RFID tags. In the case of RFID an authentication mechanism based on a cryptographic signature was developed. In spite of the simple hardware, this method allows components to be marked in a fraud-safe way while offering an offline authentication without direct access to a database. The combination of the electronic product code EPC, the unique tag ID of a transponder and the signature which is an encoded representation of these two numbers and which is stored in the RFID tag's user memory offers a secure offline solution.

Basis of the cryptographic process is an asymmetric encryption algorithm. With a private key the two arguments unique tag ID and EPC are encoded. This private key is top secret and only known by the original manufacturer. The resulting cryptographic signature is then stored in the free user memory of the RFID tag. Now the tag is marked as original. At the identification or checking point all data of the tag are read.

Via a public key all customers or users can decrypt the signature and receive the original data, which have to match with tag ID and EPC of the transponder. At accordance the tag data was originally stored by the original manufacturer (picture 3). Of course all these steps are integrated in the software of the RFID reader. Result is a data set containing the necessary information.


Manufacturer
Private key for encryption
EPC
Tag ID
+ Signature
Identification and checking point
Public key for decryption
Signature $\overset{?}{=}$
EPC
Tag ID

Picture 3 Cryptographic process steps

For transmitting these locally stored verification data sets to the central database several options are available. The system's modular design pattern is consistently maintained for this topic as well.

The modularity and transferability of the individual subsystems allows the components' genuineness to be verified not only at the customer's machine but also at any point in the supply or logistics chain. All supply chain steps which identify or check products can store and utilize this information locally or communicate it to the central server.

2.5 Data analysis and additional benefits

Thus customers, producers and retailers can at any time query the database, read up on their products' and components' history and thus gain various possibilities to fight product piracy effectively and sustainably while using all advantages of tracking and tracing.

The success of such a system depends on the long-term potential of anticounterfeiting in general but also on the concrete and fast implementation of various additional benefits for the participants – first of all for customers and manufacturers. For this reason another focus is set on the creation of services which become possible through the described system. The following examples should give an insight into these possibilities:

A machine file will be formed, which contains a list of all protected components and is supplemented with a signal light for authentication (green – "verified as original", red – "not verified"). Thus the customer or producer can quickly get an overview of a machine's current state. Further possibilities consist in detecting the usage period of specific components inside a machine or simplifying spare parts supply through accurate knowledge of the current machine configuration.

The possibility to document the use of original components allows completely new services to be implemented. Significantly better conditions and offers can be made available to quality-conscious, faithful customers through bonus programs. Customized maintenance agreements or extended warranty can be arranged in an easier and more secure way for both parties if the use of original parts can be traced.

3 Pilot installation and summary

For a better idea of the described concept a concrete example follows:

In machines for the production of deep-drawn plastic packages two chains with clips transport the processed film through the machine. The quality and measuredness of this pair of chains determine essentially the properties of the manufactured product. Among other points the influence of this component on the result of the machine led to the decision of the machine manufacturer to protect the part clip chain against product piracy with the aid of a fraud-proof mark. On the basis of the technical and economical general conditions RFID was selected as feasible marking technology. Additionally it was specified to use a small UHF transponder with loop antenna, which will be integrated in one chain link using a plastic support. The IC with EPC and tag ID includes 512 bit user memory - sufficient for the signature. Inside the machine a reader will be installed, whose two antennas registering the RFID tags are placed near the particular chain. The reader communicates with the software of the machine control. The control initiates the reading of the tag at each machine start and proves apart from the genuineness of the two chains if length and tolerance class of the built in chains comply with the specifications. Further optional functions are the storing of the period of application of the single chains and the indexing of exchange intervals.

The described protection system for anticounterfeiting allows not only for discovering copies and protecting critical machine components from product piracy. Storing the verification data in a central database allows extensive additional benefits to be offered, thus creating new services and a simplified communication between manufacturer and customer. This also helps manufacturers in their sales and service activities.
The four participating engineering companies are convinced of this. They are actively involved in the system's development and support the validation with concrete pilot installations in their companies and machines.

4 Acknowledgement

This research and development project is funded by the German Federal Ministry of Education and Research (Bundesministerium für Bildung und Forschung, BMBF) within the Framework Concept "Research for Tomorrow's Production" (fund number FKZ 02PU1143) and managed by the Project Management Agency Karlsruhe Institute of Technology.

5 Literature

[EPC-08] GS1 EPCglobal: EPCglobal Tag Data Standard Version 1.4, Ratified on June 11, 2008.

[Rei-08] Reinecke, M; Gärtner, H.; Overmeyer, L.: Schutzkonzepte gegen Produktpiraterie in der Pharmaindustrie. In: Industrie Management 6/2008. ISSN 1434-1980.

[VDM-08] VDMA: Untersuchung zur Produkt- und Markenpiraterie. Frankfurt 2008.

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

Authors

Janina Durchholz is scientific assistant at the Technische Universtät München, Lehrstuhl für Fördertechnik Materialfluss Logistik, Prof. Günthner.

Dipl.-Ing. Janina Durchholz
fml - Lehrstuhl für Fördertechnik
Materialfluss Logistik
Technische Universität München
Boltzmannstr. 15
D-85748 Garching bei München
Tel.: +49 (0)89 289-15917
Fax: +49 (0)89 289-15940
durchholz@fml.mw.tum.de

Dominik Stockenberger is scientific assistant at the Technische Universtät München, Lehrstuhl für Fördertechnik Materialfluss Logistik, Prof. Günthner.

Dipl.-Wi.-Ing. Dominik Stockenberger
fml - Lehrstuhl für Fördertechnik
Materialfluss Logistik
Technische Universität München
Boltzmannstr. 15
D-85748 Garching bei München
Tel.: +49 (0)89 289-15975
Fax: +49 (0)89 289-15940
stockenberger@fml.mw.tum.de

Prof. Willibald A. Günthner is director of the Lehrstuhl für Fördertechnik Materialfluss Logistik at the Technische Universität München.

Prof. W.A. Günthner
fml - Lehrstuhl für Fördertechnik
Materialfluss Logistik
Technische Universität München
Boltzmannstr. 15
D-85748 Garching bei München
Tel.: +49 (0)89 289-15921
Fax: +49 (0)89 289-15940
kontakt@fml.mw.tum.de