Reliable Innovative Business Model for Online Trading of Machines' Parameters in the Automation and Manufacturing Sector

Ghaidaa Shaabany[1], Reiner Anderl[2]
Computer Integrated Design Department
Technical University of Darmstadt
Darmstadt, Germany
shaabany@dik.tu-darmstadt.de[1], anderl@dik.tu-darmstadt.de[2]

***Abstract*—By new manufacturing processes, materials and/or environmental conditions new machine's parameters are needed. In general, finding the right machines' parameters of the machine is achieved by a long work effort and high costs. It is important to find the right machines' parameters of a machine to execute every manufacturing process accurately. Know-how of companies is characterized by developing the appropriate machines' parameters. A third party can develop a new business model based on a managed exchange of this know-how between companies. Thereby, an online marketplace is provided for trading machines' parameters. As a result, the revenues of these companies are increased because a new added-value is generated based on existing resources, namely, the previously developed and used machines' parameters. At the same time, the high costs of finding the right machines' parameters could be saved by purchasing them on the marketplace. These innovative ideas can be realized only by ensuring the security of the traded machines' parameters. In this paper, a reliable, innovative business model for online trading of machines' parameters in the automation and manufacturing sector is presented. It is based on the concept of B2B e-business. Thereby, it is essential to determine a usage control policy of traded machines' parameters even after purchasing. Thus, operating of these purchased machines' parameters on the machine is regulated by using different licensing models. Licenses are generated according to order's conditions for a specific machine after finishing purchasing processes on the marketplace. Before executing purchased machines' parameters on the machine, a verification process of the machine's ID and parameters' validity is required. The protection requirements over the whole trading process, as well as many security measurements for transmitting the machines' parameters to customers, are demonstrated in this paper.**

Keywords—Manufacturing processes; machines' parameters; new added-value; B2B business; usage control policy; licensing models; security; protection measurements; online marketplace; business model; electronic goods

I. Introduction

Different kinds of e-commerce marketplaces are existing and rapidly growing nowadays. They are identified according to their participants as business-to-business (B2B), business-to-customer (B2C) or customer-to-customer (C2C). B2B marketplaces are internet based platforms for trading goods between different companies, for example, between suppliers and distributors. On B2B marketplaces different business transactions are done by several companies like an exchange of products and services [1]. We focus in this paper on this kind of transactions that facilitate the exchange and distribution of machines' parameters between different companies that are working in the same field of manufacturing processes.

Many studies researched the factors that the success of a B2B marketplace depends on it. The results show that building a trust relationship with the customers is the most important factor that leads to the success of these marketplaces [2]–[4].

In our concept, the marketplace is developed to offer necessary machines' parameters for new manufacturing processes or by using special materials. Thereby, a new business model for know-how exchange between different companies is developed. At the same time, a new added-value is generated by both participants. Traded machines' parameters on the marketplace are developed from experienced machine's operators and at the same time is the intellectual property of companies. Finding the right machines' parameters for new manufacturing processes by different conditions regarding material, machines' type and the environment is an expensive process. Moreover, high costs are resulted by used material and experiment time to find these right settings of machines. The revenues of a company could be increased by offering the already developed and used machines' parameters in the marketplace. On the other side, the company that purchases these machines' parameters could save the high costs of developing them.

For a successful business model of our marketplace, it is essential to gain the trust of companies in the marketplace transactions' concept. Thus, high-security requirements are needed to meet companies' concerns regarding offered digital goods, namely machines' parameters over the transactions' process. These involve the protection of the offered machines' parameters and its confidential transmission to the customer. Furthermore, it is important to offer the machines' parameters by various possibilities for example by different use conditions and reasonable prices. To achieve this goal, a usage control policy after purchasing is required. This policy defines different utilization permissions according to the purchasing order on the marketplace. In particular, a licensing model is used to determine the different utilization permissions.

Purchasing the machines' parameters by various licenses is dealing with the problem of the intellectual property rights of companies. In this case, customers buy the rights for using these parameters on the machines instead of purchasing the machines' parameters itself. At the same time, customers are not allowed to read these parameters in plain text. Thereby purchased machines' parameters can be operated on the machine only by existing an authorized permission i.e. a valid license. That is important to ensure a clean trading process on the marketplace [5].

Machines' parameters and relevant licenses must be saved securely on the marketplace and by customers even after purchasing. Moreover, machines' parameters should be transmitted securely by means of many cryptographical methods to protect them from attacks over the internet. In this paper, we focus on the secure transmission route of the machines' parameters from the marketplace to the customer.

In the first section, many similar existing marketplaces and concepts are presented. Then needed security fundamentals like relevant protection goals and encryption methods are illustrated. The developed concept for a secure online trading of machines' parameters is presented. Thereby a secure exchange of machines' parameters and license files, as well as the security requirements by transmitting them, are given and validated. After that, the results are summarised in conclusion. In the last section, an overview of planned implementation of the concept is provided.

II. State of the Art

In this sector, many examples of existing electronic marketplaces and their respective business models will be presented. The description and the aim of these marketplaces are illustrated to give possible analogies for our concept and to derive relevant perspectives for designing our marketplace.

The marketplace Covisint is a B2B marketplace that is founded by DaimlerChrysler, Ford and General Motors. This online marketplace enables participating companies to represent their interests together, to communicate with each other and to bundle orders to achieve price and negotiation advantages through scale effects. Moreover, it enables support and interaction between manufacturers, suppliers, sellers, engineers and other stakeholders [6]. The concept of Convisit for the exchanging of companies' know-how in the automotive industry is similar to our marketplace concept in the automation and manufacturing sector.

Amazon began initially as an online bookstore and then expands its field of textiles, household goods, and electronic articles. Its platform is also open to third-party providers. Moreover, it expands its trading activities to digital content like music downloads, cloud services, video on demand and other digital services. In the age of digital media, Amazon starts trading with digital books and magazines i.e. e-books. To make this technology effectively, Amazon also developed a suitable and cheap end device named as Kindle. This Device enables downloading the purchased books directly from Amazon platform and provides them to the user [7].

By providing an e-marketplace, a digital content and suitable end devices, Amazon reduced costs and won customers for a long-term. This business idea demonstrates a good model for our marketplace concept.

Another comparable example to our marketplace is mobile apps platforms. The main idea of both of them is to offer digital goods that enable new further functions on a system [8].

As mentioned before, it is essential to provide a trustful and secure trading field by these digital platforms for acquiring a successful business model. Thus, many protection mechanisms for app provider's know-how as well as measures to protect the customers against malicious apps are established. These security mechanisms are discussed in [9]–[12].

The idea of trading machines' parameters over the internet is a fairly new concept in the automation and manufacturing sector. However, there are comparable marketplaces that are dealing with electronic goods by using several usage control policies for example in the multimedia industry. From our research in the business area, following findings are given.

The main idea of using a usage control policy for electronic goods is to offer a digital content with different utilization permissions. In this case, customers are allowed to download the content freely over the internet. However, it cannot be consumed without a valid license that includes the usage permissions [8]. Both Amazon and Adobe use this technology for their ebook ecosystems [13]. Furthermore, similar solutions are provided by Microsoft (Windows Media Audio), Apple (Fairplay) and others for controlling the use of digital audio content [14].

It is fundamental for a successful online trading of machines' parameters to establish a usage control policy of traded machines' parameters. Thus, parameters are licensed by using different security mechanisms. That is new in the industrial field and also in the automation and manufacturing sector. In our presented concept, the customer is allowed only to use purchased machines' parameters according to the terms of purchasing order on the marketplace. Moreover, the customer doesn't own these machines' parameters and is not allowed to read or copy them.

In the field of computer science, there are various methods to ensure the confidentiality, integrity and other protection goals. Several security mechanisms from the field of computer science are established to provide a trustful and secure trading environment on our marketplace. These known methods have not been implemented widely in automation and manufacturing sector.

III. Essential Fundamentals

In the following section, the fundamental basics of developing a secure concept for online trading of machines' parameters are presented. Firstly, the relevant protection goals for the presented business model are defined. Secondly, the cryptographical methods and principles that are needed to ensure these aims are demonstrated.

A. Relevant Protection Goals

Protection goals represent the protection requirements for a reliable system that must deal with electronic goods over the internet. They are necessary to make the security measurable and assessable in the context of IT security. The relevant protection goals for a clean and reliable functionality of the developed concept of our online marketplace are presented below.

1) *Confidentiality*

A call between two persons is considered confidential if it is ensured that no one else can overhear this call or get the exchanged information. In digital communication, confidentiality is achieved by using different methods of cryptography to encrypt the messages. Encryption of the message enables a protected and unreadable form of interconnected information. There are symmetrical and asymmetric encryption methods, which are presented in the following section.

2) *Integrity*

The correctness of data characterises integrity. Data should not be changed or manipulated by any unauthorized person. In a case when a message is sent from a sender to a recipient through the internet, integrity means that the recipient knows and can ensure that this message content has not been changed or manipulated during its transmission. Integrity can be applied to systems (system integrity) and software (software integrity). In particular, integrity refers to the function of the system or the software. Thereby, it is possible to ensure that the system or the software behaves exactly in the same way as the manufacturer provided. The integrity of a message can be ensured for example by a digital signature. That will be explained in detail in the next section.

3) *Authenticity*

Authenticity provides information about the origin of the message, also, to ensure that the content of this message was not changed. This means that integrity is implied in the protection goal authenticity. So, it is possible to check whether the sender of the message is also the creator of its content. It is important to distinguish between the authenticity of partners and authenticity of a message in a communication traffic. Partner authenticity means that the partners are sure about the identity of the other communication partners. Message Authentication means that the recipient of a message is sure about the identity and origin of this message. Cryptographical methods like digital signatures and message authentication codes are often used to ensure this protection goal.

4) *Non-reputability*

In the case that a message is transmitted between two parties, non-reputability ensures that it is possible to prove clearly who the author of this message is. The author can't deny the authorship of this message. That can be ensured for example by a digital signature in the web traffic. Non-reputability is essential by online trading so that the participants can not dispute about traded goods or actions.

5) *Availability*

Availability refers to the operational readiness of a system. In particular, a system should perform reliably and react correctly to users' queries within the set response time. Availability plays a major role in manufacturing, especially for IT systems that control the technical processes in the machines. Thus, it is important to protect industrial IT systems from attacks targeting their availability and operational state e.g. Denial of Service (DOS). These attacks that can cause a high damage to the company [15]–[17].

B. *Cryptography and Encryption Methods*

Cryptography aims to ensure most of the mentioned protection goals in the interconnected world. Cryptographical methods are required for secure communication between two or more parties over the internet. The encryption methods and their principles for establishing a reliable business model for online trading of machines' parameter in the automation and manufacturing sector are presented below:

a) Symmetric Key Encryption (Secret-Key-Cryptography)

Secret key cryptography algorithms are usually used to encrypt and decrypt security-critical data using the same secret key for both parties. The most important example of a symmetric cryptosystem is the Rijndael algorithm, which was standardized in the year 2000 by NIST (National Institute of Standards and Technology) as AES (Advanced Encryption Standard). Fig. 1 shows the symmetric key encryption/decryption of a message by sender and recipient using the AES cryptosystem.

By symmetric key encryption system, a sender encrypts the data, and the recipient decrypts it by using the same secret key. That is described in the following formulas:

Symmetric encryption of a message:

$$\mathrm{c_i} = \mathrm{AES}(\mathrm{K}\,;\mathrm{m_i}) \tag{1}$$

Symmetric decryption of a message:

$$\mathrm{m_i} = \mathrm{AES}^{-1}(\mathrm{K};\mathrm{c_i}) \tag{2}$$

m_i : message K : symmetric key c_i : cipher

Symmetric key encryption systems perform simple and very fast. However, there are many problems regarding the secret key exchange processes as well as regarding the high number of shared keys for all communication partners that should be secured. Thus, it is important to find a secure transmission way for exchanging secret keys between communication partners by this symmetric key encryption. If an encrypted message and its related secret key be hacked during its transmission over the internet, the protected content of this message isn't secured anymore [15]–[17].

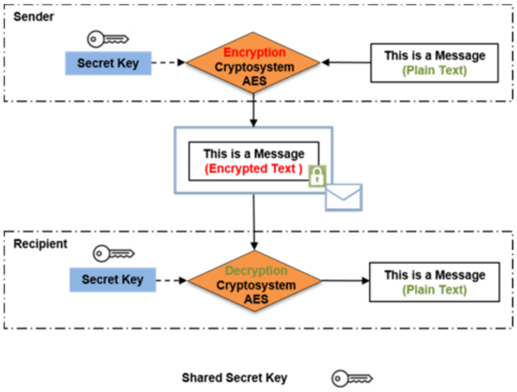

Fig. 1. Symmetric key encryption AES.

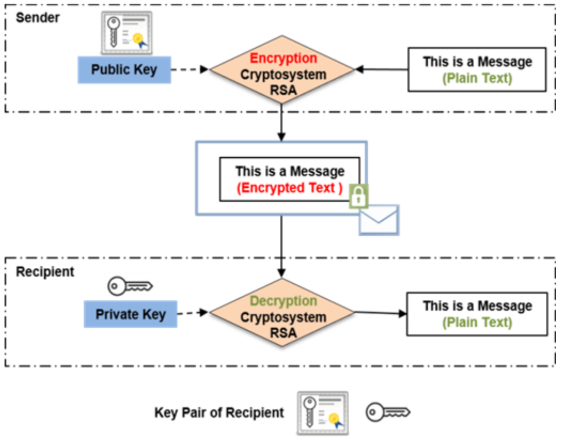
Sender
Public Key
Encryption Cryptosystem RSA
This is a Message (Plain Text)
This is a Message (Encrypted Text)
Recipient
Private Key
Decryption Cryptosystem RSA
This is a Message (Plain Text)
Key Pair of Recipient

Fig. 2. Asymmetric key encryption RSA.

b) Asymmetric Key Encryption (Public-Key Cryptography):

Asymmetric key encryption systems normally use two keys: a private secret key and an associated public key. These two keys are referred to each communication partner and known as a key pair. In particular, the message is encrypted by a sender using the public key of the recipient. This message can be decrypted only by using the recipient's private key. The most known asymmetric key encryption system is RSA (according to R. Rivest, A. Shamir and L. Adleman) cryptosystem. A description of RSA functions is shown in Fig. 2.

By asymmetric algorithms, it is impossible to derive the associated private key from a public key in case that it is hacked from a potential attacker. As a result, the key exchange problem by a symmetric key encryption is solved. The encryption and decryption operations of a message by RSA cryptosystem are described in the following formulas:

Asymmetric encryption of a message:

$$c_i = \mathrm{RSA}\ (e, m_i) \quad (3)$$

Asymmetric decryption of a message:

$$m_i = \mathrm{RSA}^{-1}(d; c_i) \quad (4)$$

m_i : message e: public key of the recipient

c_i : cipher d: private key of the recipient

Disadvantageous of an asymmetric key encryption compared to symmetric encryption systems is that the system's operations are about a factor of 1,000 slower than by the symmetric encryption systems. Thus it is very complicated and expensive to encrypt large amounts of data using asymmetric algorithms [15]–[17].

c) Hybrid Key Encryption

By Hybrid Key Encryption, the symmetric and asymmetric key encryption is combined. Advantages and disadvantages of both methods are ideally complemented. As mentioned before, the problem with symmetric key encryption is by exchanging of the secret key. This is solved by hybrid encryption through generating a random key for the symmetric encryption.

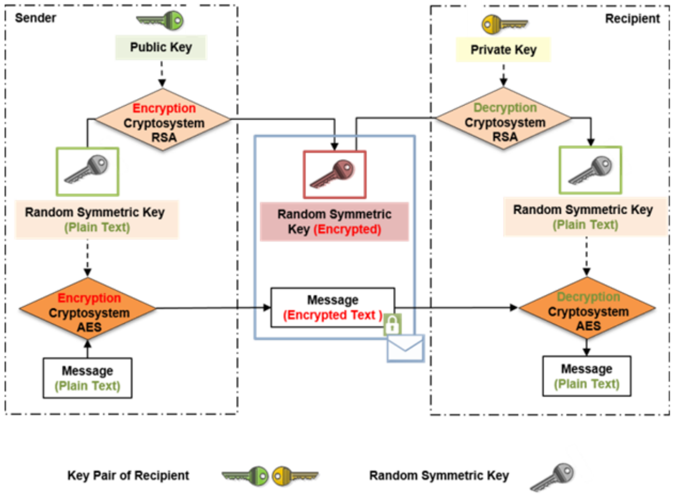
Sender
Public Key
Encryption Cryptosystem RSA
Random Symmetric Key (Plain Text)
Encryption Cryptosystem AES
Message (Plain Text)
Random Symmetric Key (Encrypted)
Message (Encrypted Text)
Recipient
Private Key
Decryption Cryptosystem RSA
Random Symmetric Key (Plain Text)
Decryption Cryptosystem AES
Message (Plain Text)
Key Pair of Recipient
Random Symmetric Key

Fig. 3. Hybrid key encryption.

A sender uses this random key for encrypting the message that could have a large amount of data. Subsequently, the sender encrypts this random key asymmetrically with the public key of the recipient. Then, the encrypted message as well as the encrypted random key are sent to the recipient. After receiving the message, the recipient decrypts first the symmetric random key with his private key. After that, he uses this key to decrypt the message that was decrypted symmetrically.

Fig. 3 illustrates the principles of a hybrid key encryption that often uses in practice RSA and AES as an asymmetric and symmetric encryption system.

Moreover, the operations by a hybrid key encryption are described using the following formulas:

Symmetric encryption of a message:

$$c_i = AES(K; m_i) \quad (5)$$

Asymmetric encryption of a random key:

$$\mathrm{K}_c = \mathrm{RSA}\ (\mathrm{e}, \mathrm{K}\ ) \quad (6)$$

Asymmetric decryption of a random key:

$$\mathrm{K} = \mathrm{RSA}^{-1}(\mathrm{d}; \mathrm{K}_c) \quad (7)$$

Symmetric decryption of a message:

$$m_i = AES^{-1}(K; c_i) \quad (8)$$

m_i : message K : random symmetric key

c_i : cipher e : Public key of the recipient

K_c: encrypted key d : Private key of the recipient

Hybrid encryption algorithm will be used for ensuring the confidentiality of traded machines' parameters on the marketplace. This is important to ensure the confedintiality of the machines' parameters.

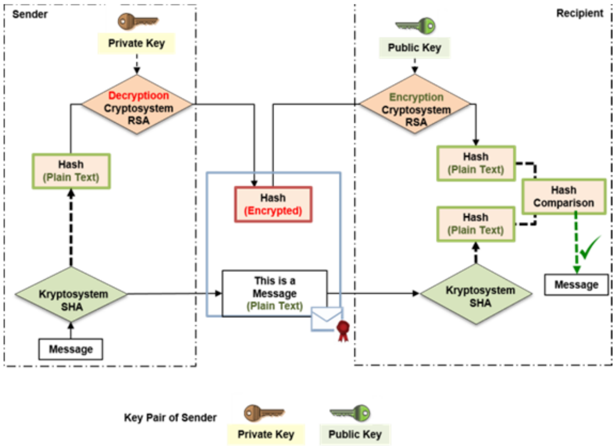

Fig. 4. Digital signature.

d) Digital Signature

The digital signature is used to prove the identity of a sender of a message that is sent electronically. Also, digital signatures ensure that the content of this sent message has not been changed after sending it. The sender generates a hash value of the message and then encrypts this value with his private key. Then the encrypted hash value is attached as encrypted information to the sent message. The sender sends the message with the attached encrypted hash to the recipient. This encrypted information can be decrypted and read only by using the associated public key of the sender.

The recipient generates a hash value of the received message using the same hash system that the sender used to generate the hash value of the message. At the same time, the recipient decrypts the encrypted hash using sender's public key. By comparing these two hash values, the recipient can ensure if the content of the sent message has been changed after sending it and if it has been sent from the sender who signed it. These can be ensured when the two hash values are identical. The function of the digital signatures is described in Fig. 4.

The digital signature is significant in the digital world since attackers can easily falsify the electronically transmitted messages. It is essential that authenticity of digital signatures can be verified and that digital signatures cannot be falsified. Moreover, a digital signature should not be transferable from one document to another. Furthermore, digital signatures should be regularly checked for transmitted messages to ensure the correctness of the message content and its origin [15]–[17].

e) Transport Layer Security TLS

Nowadays there are several known security protocols, such as Transport Layer Security (TLS). These protocols are needed to secure connections between two computers and in particular between a server and a client by each web traffic. TLS is the follower version of Secure Sockets Layer (SSL) and hybrid encryption protocol. These standards provide a protocol for encrypting of data and for ensuring the identity and integrity over the internet. In the first step, TLS negotiates over a handshake protocol, which is used to exchange the supported cryptographic methods "cipher suites" and session keys between the participants (see Fig. 5).

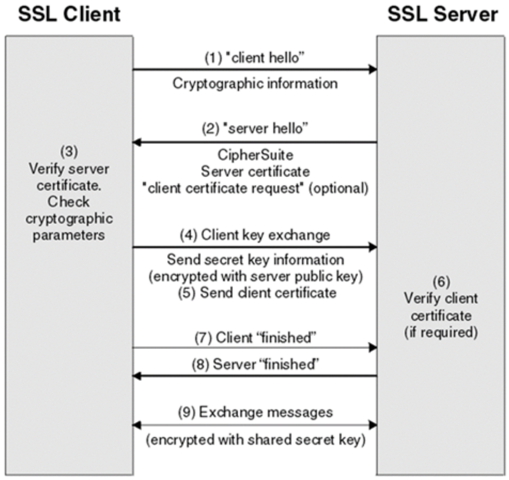
SSL Client
SSL Server
(1) "client hello"
Cryptographic information
(2) "server hello"
CipherSuite
Server certificate
"client certificate request" (optional)
(3)
Verify server certificate.
Check cryptographic parameters
(4) Client key exchange
Send secret key information
(encrypted with server public key)
(5) Send client certificate
(6)
Verify client certificate
(if required)
(7) Client "finished"
(8) Server "finished"
(9) Exchange messages
(encrypted with shared secret key)

Fig. 5. Overview of the SSL/ TLS handshake [18].

Moreover, certificates can be exchanged to verify the authenticity of the parties. This step is optional for a client. Otherwise, a server authenticates itself and sends a selected cryptographic method from the cipher suite. Then the client checks the server certificate [17]. After that, a session key between server and client is exchanged. There are two options for generating this key: the client sends the server a random key, which is encrypted with the server public key. Alternatively, both parties calculate a common secret key using the Diffie-Hellman key exchange method. After that, all transmitted messages are encrypted and decrypted using this session's key.

If the handshake has been terminated successfully, TLS starts the record log that ensures confidentiality and integrity of data. This protocol divides the message into blocks of the same size, which are encrypted and compressed using the determined method in the handshake protocol. Then, the messages are sent together with an overhead of metadata. These metadata are required for verifying the integrity of the messages. Finally, received messages are decrypted, verified, decompressed, and reassembled by the recipient. In case the transmission fails, TLS notifies both parties via alert protocols about the error log.

The agreed encryption method from the cipher suite is maintained throughout the whole session, regardless of the connections' number. The sessions' term should be maximum 24 hours long, and then a new key should be negotiated. The standard TLS is deliberately made open and allows the participants to use any method of cryptographic algorithms for a connection. Thus, TLS remains valid even if new algorithms offering higher security and efficiency will be used [15]–[18]. From previous findings, TLS protocol is a secure internet protocol that ensures a reliable transmission of our machines' parameters in our concept of the online marketplace.

IV. Reliable Concept for Online Trading of Machines' Parameters

The concept for a secure data transmission from the marketplace to the customer is presented in this section. The main goal is to protect the traded machines' parameters on the marketplace from against misuse and manipulation. A data flow diagram is shown to visualize the possible attack points and areas. Moreover, three main stakeholders and their trust limits are represented by different colors (see Fig. 6). Each stakeholder has different security needs and infrastructure, such as certificates and cryptosystems that are used for encryption, decryption, and signing the transmitted data.

Two possible types of attackers are conceivable in our scenario of online trading of machines' parameters. The first potential type of attacker comes from the outside, who tries to access the machine via the internet or listens to the data stream between the server of the marketplace and the customer. The second potential type of attacker comes from inside, who has physical access to the machine by the customer and as a result to the purchased machines' parameters. The workflow that describes the scenario of trading machines' parameters on the marketplace is shown in Fig. 6.

The provider prepares the machines' parameters before offering them on the marketplace in one package for transmitting them to the marketplace. Transmitted package is divided into two different files; the sensitive data that have to be protected (namely, offered machines' parameters) and the related metadata (e.g., material, machine type, etc.). The file of machines' parameters contains the know-how of the provider, and therefore it must be confidentially transferred. The metadata files are not a sensitive information and do not have to be transmitted confidentially since they include environmental conditions and needed information for generating the relevant CNC-code of the machine.

The provider signs the prepared package with the mentioned two files of data electronically before offering his machines' parameters in the marketplace. The provider specifies desired prices according to the terms of use and then uploads them to the marketplace.

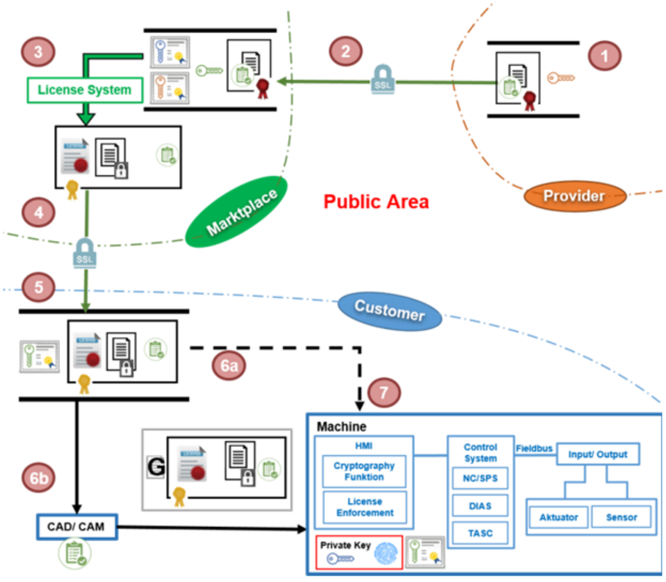

Fig. 6. Workflow of trading of parameter sets.

After a purchase process has been completed, a license file is created by the licensing system in the marketplace according to the selected usage permissions by the customer. These are encapsulated with the two mentioned files in one package and signed electronically by the marketplace. Then, this package is sent either directly to the customer or stored on the server by the marketplace. The purchased parameters' set and the associated license will be available for download on the need in the marketplace. Once the data package arrives by the customer, it will be transferred either directly to the machine or the CAD/CAM workstation. The machine's parameters can be only decrypted and executed on the machine, whereby CAD/CAM engineer can read the metadata that is necessary for generating of needed CNC-code. Moreover, the identity of the machine must be verified, and after that, the parameters can be decrypted.

The license file involves the usage permissions and provides the required key for encrypting the parameters' file as soon as it is still valid. After every operation process of the parameters, the machine should send an update of the license. At the same time, it is necessary to check the validity of license by each use of parameters' file to warranty the provided usage control policy. If the usage authorization is aborted, the machine can no longer decrypt and operate the purchased machines' parameters. In the case of further need for machines' parameters, the customer must request a new license on the marketplace.

In the next section, various security measures for ensuring the relevant protection goals assigned by different stakeholders are demonstrated in Fig. 7. Moreover, the significance of these protection goals by every stakeholder and needed protective measures for a secure online trading of machines' parameters are illustrated.

1) *Confidentiality*

The confidentiality of transmitted machines' parameters is interesting primarily for the provider since hackers could threaten his know-how, e.g. while uploading the data package to the marketplace. This problem also affects the business model of the marketplace very much, because traded machines' parameters could be attacked and used by unauthorized persons. Thereby, no one has more interest in purchasing offered machines' parameters on the marketplace because these parameters can be got for free. An internet security protocol is used for data transmission from the provider to the marketplace to ensure data confidentiality, for example the previously described TLS/SSL protocol. In our suggested scenario, the marketplace is considered as a trustful platform; therefore the valuable machines' parameters are uploaded without encryption and can be stored on the server of the marketplace in plain text.

However, machines' parameters will be encrypted and then transmitted to the customer to ensure the confidentiality of these parameters after completing the purchasing process.

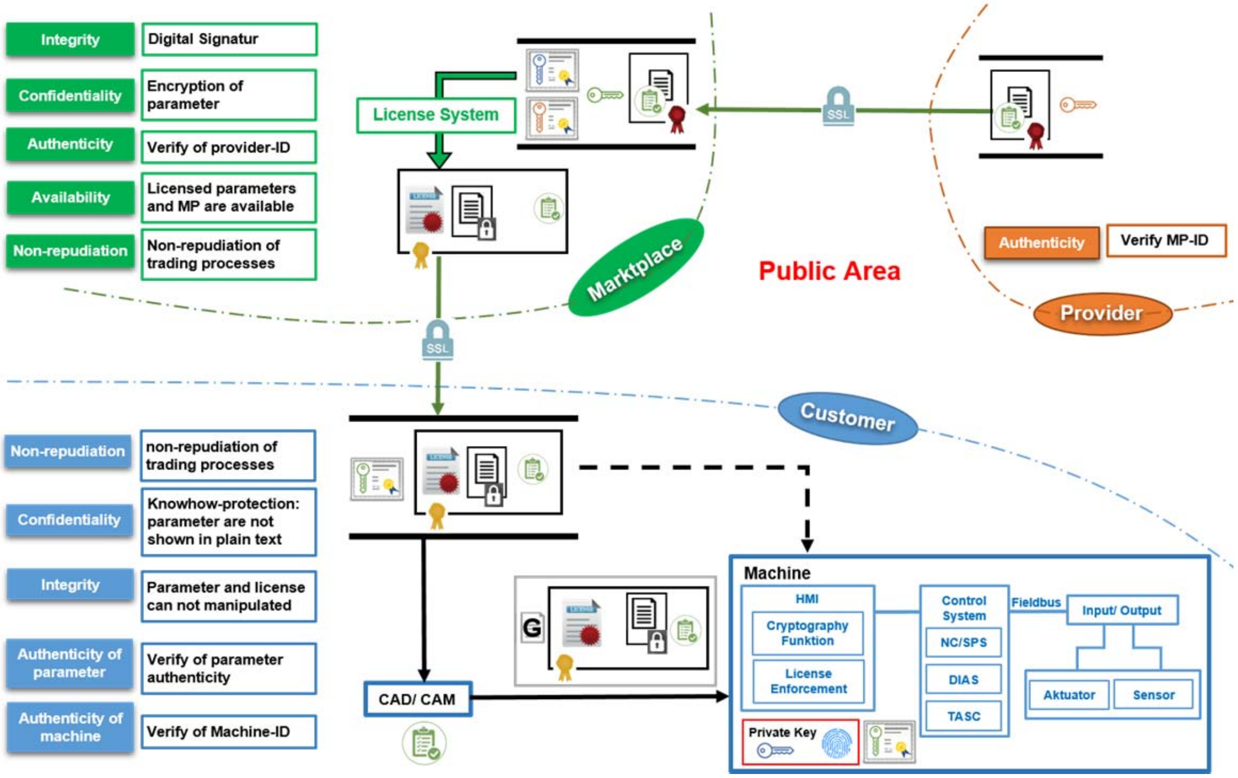

Fig. 7. Secure transmission path of Parameter sets.

As mentioned before, a cryptosystem with hybrid key encryption is used for encryption data package before transmitting it to the customer.

The significance of confidentiality by the customer is different. It is essential to protect the know-how of the parameters' provider even after purchasing of machines' parameters on the marketplace. If a customer could read the purchased machines' parameters, he would have the possibility to buy these parameters for one-time use and then to copy and save them for further uses by similar manufacturing processes. It is essential for the success of the marketplace business model that a customer is only allowed to operate the purchased machines' parameters on the machine. Although the customer has no rights to view these machines' parameters in plain text. Therefore, the values of these parameters are not displayed on the machine by the customer in plain text. At the same time, the customer is allowed to adapt these parameters only by increasing or decreasing some of them within a specific area. In case that mentioned protective measures regarding confidentiality of traded parameters are implemented, the machines' parameters are secured from unauthorized utilization and are protected from outside as well as from inside attackers.

2) Integrity

The marketplace must ensure the integrity of traded machines' parameters in order to ensure the promised security of offered digital goods. It is also necessary to prevent sending manipulated parameters into the machine by a customer because it could cause great damages. Two steps ensure that. First, it is important to sign the machines' parameters electronically by the provider before uploading them to the marketplace. The functionality of a digital signature was described in the second section. The integrity of the uploaded machines' parameters is verified then on the marketplace using the public key of the provider. Public keys of all participants are managed and stored in the database of the marketplace.

Second, the integrity of machines' parameters and related license file has to be ensured by the customer. Thus, it is essential to ensure that the content of a license can't be changed or manipulated by customers. Therefore, an integrity check of license file by the customer is required before encrypting the machines' parameters. Thereby, an unauthorized utilization of machines' parameters by customers is excluded. At the same time, customers must be prevented from changing the content of the license file, for example, the end date of use permissions.

3) Authenticity

The providers of machines' parameters should prove their identities before starting any trading process on the marketplace. There are several known methods for ensuring the authenticity of communication partners, e.g. by a call, by a personal code and/or by using hardware as a smart card or a token. Also, a proof of the machine's identity is required for enabling a successful license management and usage control policy, as licenses are created for a specific machine that is owned by a specific customer.

For the provider, it is also important to check the identity of the marketplace before offering the machines' parameters. For this purpose certificates with a specified identity and relevant keys for the marketplace are required.

The most important content of these certificates is the public key of the marketplace that should be sent to all participants. However, to guarantee the authenticity of these certificates, they could also contain information about the web address or the owner e.g. company name. A digital signature is also attached in these certificates. Central authorities, so-called "Certificate Authorities" (CA) generate and sign the certificates for public servers [10].

4) Non-repudiation

Non-repudiation ensures that the seller owned the machines' parameters before starting the purchasing process and after that the customer owns them, which means that both parties can't dispute this awareness later. It is essential for the marketplace to know and proof the origins of traded machines' parameters. Therefore all participants must authenticate themselves during the registration process on the marketplace and should sign in before offering or ordering any parameters' set. Before utilizing the parameters on the machine by the customer, the origin of this parameters' set must be verified, i.e. The digital signature of the marketplace should be verified by the customer. Since the digital signature is based on the private key of the sender that only has access to it. That allows the marketplace to be uniquely identified. Thus, the marketplace, as well as the provider, can be uniquely identified by every trading process. That is essential to prevent repudiation between partners by our business model.

5) Availability

The platform services must always be available to the participants to fulfill the sense of the presented marketplace. Management of traded machines' parameters and related licenses must be carried out and downloaded without hindrances. Above all, the availability of the licenses of purchased machines' parameters on the marketplace has to be always guaranteed for customers by need. That means that the customer can call up the license at any time over the internet in order to utilize the purchased parameters' set on the machine.

V. Conclusion

We presented in this paper a concept for a new innovative and secure business model in the field of e-business in the automation and manufacturing sector. This concept illustrated a marketplace that enables online trading of machines' parameters for new manufacturing processes or special materials. It based on the exchange of manufacturing's know-how between companies and to enhance its productivity and at the same time to increase companies' revenues. The workflow of the trading process of the machines' parameters on the marketplace is demonstrated. In the developed concept the machines' parameters are managed, offered and transmitted by the marketplace that provides a high level of security to ensure the confidentiality and integrity of the traded machines' parameters. The required protection goals and many needed cryptographical methods are explained that are important to realize a reliable concept for online trading of machines' parameters in the automation and manufacturing sector. The significant protection goals are cleared and ensured for the developed concept. The whole transmitting path of machines' parameters from the provider to the marketplace and then to the customer was secured by means of different protection measures.

VI. Future Work

The developed concept for a reliable trading of machines' parameters on an online marketplace will be implemented in our labor at the University. Within a students' project, a liquid mixer was made that needs several machines' parameters for different recipes of mixing drinks. The machine is connected to the internet to the marketplace that offers several machines' parameters, namely, recipes. Many measures for enabling an effective usage control policy of the offered machines' parameters will be researched. Moreover, to ensure relevant protection goals, different protection measures will be implemented, compared and evaluated. This concept will be then adapted to provide an efficient and secure concept for the trading of machines' parameters in the automation and manufacturing sector.

Acknowledgements

This work has been funded by the German Federal Ministry of Education and Research (BMBF) in the project IUNO – National reference project on IT-Security in Industrie 4.0 (project number 16KIS0328).

References

[1]. W. Thitimajshima, V. Esichaikul, und D. Krairit, "Developing a Conceptual Framework to Evaluate Public B2B E-Marketplaces", in PACIS 2015 Proceedings.

[2]. S.-H. Chien, Y.-H. Chen, und C.-Y. Hsu, "Exploring the impact of trust and relational embeddedness in e-marketplaces: An empirical study in Taiwan", Ind. Mark. Manag.Bd. 41, Nr. 3, S. 460–468, Apr. 2012.

[3]. B. A. Kumar, "Cogniton Based Trust Model for B2B E-Market", gehalten auf der 2015 1st International Conference on Next Generation Computing Technologies (NGCT), Dehradun, India, 2015.

[4]. S. A. K. Beige und F. Abdi, "On the critical success factors for B2B e-marketplace", Decis. Sci. Lett., Bd. 4, Nr. 1, S. 77–86, 2015.

[5]. G. Shaabany, M. Grimm, und R. Anderl, "Secure Information Model for Data Marketplaces enabling Global Distributed Manufacturing", Proc. 26th CIRP Des. Conf., Juni 2016.

[6]. S. Schau, "Covisint – Accelerating the pace of business", in B2B-Erfolg durch eMarkets und eProcurement, M. Nenninger und O. Lawrenz, Hrsg. Wiesbaden: Vieweg+Teubner Verlag, 2002, S. 313–324.

[7]. M. Jaekel, Hrsg., "Die Anatomie digitaler Geschäftsmodelle". Wiesbaden: Springer Fachmedien Wiesbaden, 2015.

[8]. W. Rosenblatt, S. Mooney, und W. Trippe, "Digital rights management: business and technology". John Wiley & Sons, Inc., 2001.

[9]. Google, "Android for Work Security White Paper". 2015.

[10]. Google, "Google for Work Security and Compliance Whitepaper". 10-Nov-2016.

[11]. D. A. Dai Zovi, "Apple iOS 4 security evaluation", Black Hat USA, Bd. 24, S. 37, 2011.

[12]. Egners, B. Marschollek, und U. Meyer, "Hackers in your pocket: a survey of smartphone security across platforms", RWTH Aachen Tech Rep AIB-2012-07, 2012.

[13]. M. M. Azad, A. H. S. Ahmed, und A. Alam, "Digital rights management", Int. J. Comput. Sci. Netw. Secur. Bd. 10, Nr. 11, S. 24–33, 2010.

[14]. R. Hammersland und J. Strømstad, "Digital Rights Management", 2008.

[15]. Eckert, "IT-Sicherheit, Konzepte – Verfahren – Protokolle", München, 2013.

[16]. J. Buchmann, "Einführung in die Kryptographie", 6, Überarbeitete Auflage., Berlin; Heidelberg: Springer Spektrum, 2016.

[17]. S. Spitz, M. Pramateftakis, und J. Swoboda, "Kryptographie und IT-Sicherheit, Grundlagen und Anwendungen", Wiesbaden: Vieweg+Teubner Verlag, 2011.

[18]. W. Stallings, "SSL: Foundation for Web Security", Bd. 20, 1998.