A Secure Electronic Market for Anonymous Transferable Emission Permits

Markus Gerhard [1], Alexander W. Röhm [2]
[1]*University of Gießen, Germany;* [2]*University of Essen, Germany;*
Markus.Gerhard-1@wirtschaft.uni-giessen.de; roehm@wi-inf.uni-essen.de

Abstract

Electronic Markets as new mechanisms for co-ordinating allocation of goods, are supposed to reduce the trading immanent transaction costs, especially when the traded goods are digitally represented. A market with no transaction costs is theoretically the most efficient possible allocation mechanism.

The US government has recently passed the Acid Rain Act, which uses a system of tradable permits to reduce pollution for the first time. In this document we present a new example of a solution for environmental policy with tradable emission permits, that is based on electronic markets. Open electronic markets are able to improve a systems efficiency by solving the difficulties that result from high transaction costs. We introduce the concept of original and anonymous permits, which can be freely traded in a open network without any restrictions. It may be used for other types of electronic documents such as shares, which are only of value, if they satisfy the criteria "Originality". The advantage of anonymity is of an economic nature, especially in terms of acceptance of the open electronic market.

An open electronic market in an open network like the Internet is insecure, but it is accessible for a large amount of potential users. To get a open network, where trading is without restrictions, and which is also secure, a set of security services have to be provided.

In this work we specify a secure completion phase of an electronic market for free tradable, anonymous and original permits by using cryptographic methods and organisational measures such as digital signatures and trusted third parties. We proposed this in [12] too.

1 Introduction

Human interventions in nature has caused a level of pollution near or even beyond the limits of capacity of many environmental systems. The green-house effect, dying forests and the pollution of air, water and land by various harmful substances are presently the most popular examples of nature's extended exploitation by human beings. Therefore, people increasingly demand an environmental policy which is orientated towards the vision of Sustainable Development. From the anthropocentric point of view, this means to work towards the preservation of the environment as the irreplaceable foundation of each socio-economic system for our future generations.

Up to now, practical environmental policy in the Federal Republic of Germany and many other western industrial countries has mainly been based on direct-controlled strategies [11] to attain a predetermined set of environmental standards. However, this approach to the issue has been looked at critically by many economists. They postulate these instruments are characterised by a lack of ecological effectiveness and economic efficiency and therefore call for a change of environmental policy instruments in favour of market based strategies. One of the most popular examples of this environmental economic approach is the concept of tradable emission permits, which was put into practice for the first time within the framework of the Clean Air Act in the United States. The theoretical analysis of this concept leads to positive results, for it offers the opportunity to achieve specified environmental targets at least costs for the society. Furthermore, there's the possibility to induce incentives for the innovation and implementation of environmental protection techniques. However, economic efficient solutions by these means require a mechanism that co-ordinates the allocation at no or at least low transaction costs [9]. The reason for this is that on a market for tradable permits low transaction costs will lead to an increased transaction volume (when we suppose diverse cost structures of the pollution industry) and in this way to increased economical efficiency.

Electronic markets in open networks like the Internet, just offer the possibility of co-ordinating allocation of goods at low transaction costs. Although this hasn't been empirically proved yet, we share this view especially with regard to the trade of digital products and hence call for a forced political accomplishment of the model of tradable emission permits. An electronic market should be defined as a market in which products are traded, and which is realised by information technology to support

1060-3425/98 $10.00 (c) 1998 IEEE

all phases of the buying process (information phase, arrangement phase and completion phase) [32].

In this work we elaborate the technical requirements for an electronic market for tradable emission permits. We do so by specifying a system in which an electronic market as co-ordinating mechanism will put the model of tradable emission permits into action. For realising a free, sure and efficient trade with emission permits in our system, we suggest the concept of original and anonymous licenses.

First, we will explain the model of tradable emission permits in chapter 2. In chapter 3, we will discuss the necessary requirements for realising an electronic market and then specify the concept of original and anonymous licenses in chapter 4. This will be followed by a discussion of the organisational surroundings in chapter 5. Finally, we will judge the specification and give a general outlook of future perspectives.

2 The Model of Transferable Emission Permits

The basic idea of Dales' and Crocker's [7, 6] model of transferable emission permits is to create markets for the allocation of environmental goods. Generally, we presume the existence of property rights as a necessary condition for the markets' ability to function. However, to presume existing property rights for environmental goods, it has to be considered that these goods are collective and therefore not institutionalizable. Therefore property rights for environmental goods have to be related to specific types of environmental exploitation, such as an exactly quantified amount of environmental pollution.

In the model of transferable emission permits, Government defines a specific environmental quality target for a certain environmental system, e.g. a lake, by using certain criteria. These criteria may be based on economic profit-cost analysis (to attain an optimum environmental quality), or they may be based upon the criteria of sustainability, stating that pollution should not be beyond the limits of the assimilation capacity of an environmental system. Having fixed the environmental target, the corresponding maximum emission quantity can be defined. This emission quantity is divided into regional emission contingents for each harmful substance of a certain region. The various emission contingents for each substance are documented in emission permits and licenses. Pollution is only allowed for owners of corresponding permits which exactly define the allowed quantity of pollution, the polluting substance, the affected region and the period of time. The first allocation of emission permits for polluters can be provided by means of auction, sale at a fixed price by government, or by means of free allocation (the Grandfathering method). According to many authors of economic literature, the Grandfathering method is to be preferred due to a higher level of economic and political practicability: First, emission permits are allocated among established polluters by government. Second, the politically fixed environmental target is attained by the devaluation of emission rights. And third, the further allocation of emission permits is ruled by laws of demand and supply, which means that emission permits are freely tradable in each region. As a result free markets with pricing for emission permits arise.

Presuming that companies of polluting industries use the criteria of minimum individual costs when being faced with the issue of avoiding emissions, they will buy emission permits when their individual marginal avoiding costs (costs for measures taken to reduce emissions) are higher than the price of permits. In instances where the price of permits is higher than the individual marginal avoiding costs, they will initiate measures for environmental protection. This means that the individual polluting company will buy emission permits until its individual marginal avoiding costs are equal to the price of permits. The economic result is that a politically fixed environmental target is realised at least costs to the society: Emission permits will be owned only by those companies which face the highest avoiding costs whereas measures for protecting the environment are taken only by those who have the least costs with it. The mechanism is adaptable to changes of environmental targets, which means that there's the possibility to tighten environmental targets (e.g. in case of a new ecological insight or discovery) by the devaluation of emission permits.

The theoretical judgement of emission permits for environmental protection is generally based on three criteria:

- Criteria of ***Ecological Effectivity*** examines the extent to which a political instrument realises a predetermined ecological target surely, fast and lastingly.
- Criteria of ***Economic Efficiency*** evaluates if the instrument will realise a fixed environmental target at least costs for the society
- Criteria of ***Innovative Efficiency*** examines if the instrument potentially induce environmental technical innovation, as this will offer the opportunity to reach the same environmental targets at lower costs, or to realise higher environmental targets at the same costs.

The judgement of emission permits against these criteria leads to remarkably positive results. With respect to the Ecological Effectivity it can be noticed that predetermined environmental targets are generally realisable, because the number of permits in public is restricted to the fixed environmental standard, which in this way is ensured - presuming that all individuals act legally. This means that ecological efficiency can be expected to a high level when implementing adequate measures of control and sanction. Economic Efficiency can be realised as well: A rational polluters will avoid emissions as long as his avoiding costs (marginal costs of an avoided emission unit) are lower than the emission permits' price. Presuming workable markets and the non-existence of transaction costs, this rational behaviour leads to a distribution of environmental protection measures among the polluters at minimum costs for the society. Moreover, incentives for environmental technical innovations are permanently encouraged, for the polluting industry will aim at minimum costs for emission permits. Besides the chance to minimise costs, there's the chance to make profit by selling emission permits which are not used any more due to a higher environmental technical standard. These two effects may be labelled the general economic incentives for innovation. Innovation leads to a shift of a society's marginal avoiding cost function to the left, which means that the same environmental standards are realisable at lower costs, or that higher environmental standards can be reached at existing costs. However, the improvement of techniques to avoid emissions may lead to a lower demand for emission permits and therefore to a lower price, which in return will reduce the incentive effects of emission permits. This effect could be avoided by the government's buying-up and devaluation of emission permits, as well as by a reduced renewal of periodically restricted emission permits.

Taking the theoretical capability of emission permits into account, one may wonder why this concept is currently only hesitatingly implemented into political practice. From the environmental policy maker’s point of view, this is due to a lack of reality of the simplified model, which means that important real conditions haven't been taken into consideration sufficiently yet. However, economists increasingly take these conditions into account. For example, they examine the main problem of transaction costs whose absence is a necessary condition for the success of the model. Transaction costs occur for the initiating, negotiation, completion and the control of contracts. According to empirical studies, these costs are very high on markets for emission permits, which is due to a lack of technical and marketing transparency. Hence the exchange possibilities provided by the market can only be used insufficiently [20]. However, there's the possibility to reduce transaction costs and in this way to improve the workability of a market for tradable emission permits by the trade on electronic markets. In the following chapters, we're not aiming at proving this, but at illustrating how this might work.

3 Technical Requirements

It was Malone, Yates and Benjamin, who first stated in 1987, that the fusion of telecommunication and computer technology will cause in some areas a shift from hierarchies to markets as co-ordinating mechanisms. They argued, that transaction costs of electronic markets will reduce more than the transaction costs of electronic hierarchies [19]. Nowadays their arguments are commonly accepted.

Some areas of trading seem to be more suitable than others. In the Internet you can find some very successful examples like bookstores (www.amazon.com; www.books.com) or travel agencies and airlines (www.ltu.de; www.british-airways.com). What is the secret of successful Internet shops? One of the big advantages is the products’ simplicity. To compare the different offers you only have to know a few facts or parameters and the price. Tradable rights like the emission permits used in this work do have the same advantages. Besides that you can represent them fully as digital documents - if we assume that legal circumstances are sufficient. This again lowers transaction costs in the completion phase, because the digital documents can be delivered over the network.

Why are such markets so rare on the Internet? What are the reasons, that make users hesitant? Actually users tend to use electronic markets also for tradable rights in the Internet. But there are deterrent circumstances for the users. Mainly the lack of data security, missing privacy and unclear legal situation concerning electronic trading hinder its growth [33]. It is our goal to specify an electronic market for emission permits, which satisfies the described criteria, Ecological Effectivity, Economic Efficiency and Innovative Efficiency.

This goal can only be reached together with data security, privacy and clear legal regulations, because this is the only way to obtain the acceptance of the acting people (politicians, authorities, emitter etc.). In economic theory a efficient market has to fulfill several criteria [8]. Some of these criteria imply, that a sufficient number of participants are present at the electronic market. What guides us to the property of an electronic market, that it should be open to all, who want to participate. For example environmentalists should be able to buy and sell emission permits like the polluters can. Indirectly this entails, that the citizens preferences play a bigger part. An open market structure is therefore seen as the better solution in terms of electronic market efficiency. It is freely accessible to all and it gains the users acceptance. The Internet provides with its open structure a platform where a large number of potential participants can join the electronic market [13].

However, because the Internet has this open structure, it is also insecure. And the resulting security threads have to be addressed with adequate security services. Besides the elementary risks: loss of confidentiality, integrity and authenticity of sent messages, in this context of tradable emission permits the risk of loosing the originality has to be addressed, because a permit can potentially be copied and used multiply. To redress these risks and to guarantee users security is an important topic of this work.

Ensuring data security is not the only way to gain users acceptance of electronic markets for tradable emission permits. Another way is to extend privacy by realising anonymity of the licences. Various grades of anonymity are known [26]. In this context anonymity means: By knowing the emission permits data one can neither find out the actual nor the former owner's identity. Furthermore the emission permit contains no information about the amount of toxins the owners really emitted - as far as no emission above allowed limits occur. Anonymity may be in the toxin emitting industries interest, because their image depends more and more on environmental issues. On the other hand environmentalists can buy emission permits to reduce total emission. Anonymity protects them from being put under pressure by other lobbyists. So they can have free influence on the environmental quality. A disadvantage of anonymity probably is, that it may support financially strong and powerful companies, who try to eliminate competitors by buying all emission permits. However, this behaviour will be the same and will have the same consequences without anonymity, since buying through others or the use of pseudonyms would support this behaviour in the same way.

One of the important parts of environmental policy is the realisation of an appropriate surveillance. To find an appropriate way to control wether anybody illegally emits toxins or not is a trade off between costs and the completeness of control. Complete control which leaves no gap for illegal emission is very expensive, while insufficient control leads to illegal emission and the system proves ineffective in reaching the environmental goal. Each implementation of environmental policy needs therefore a technology for control of emissions. In this proposal we describe a possible way.

Economic Efficiency of the system depends on its costs and acceptance, whereas *Ecological Effectiveness* is only achievable if no forged or illegally copied emission permits are put in circulation. A means to get *efficiency of innovations* is the limited validity of the emission permits.

Valid emission permits in their digital form sometimes have to serve as evidence in a legal proceeding. To get a legal binding of digital documents technical measures are not sufficient.

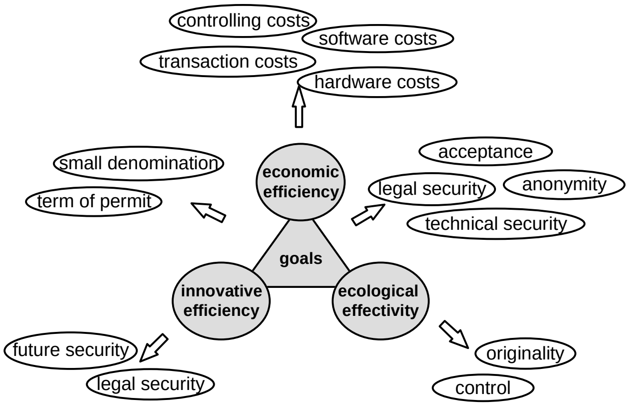

Figure 1. Goals of the realisation

It is also necessary, that the technologies work together with organisational measures and laws. In the Federal Republic of Germany the new digital signature act provides the legal basis. The realisation has to be embedded in the certification authority infrastructure that this digital signature act is applicable. Figure 1 summarises how we derived the technical requirements from the overall goals of environmental policy. Given the complexity of a cost analysis, a further analysis is not included in this report.

4 Anonymous original licences

In this chapter we present a possibility, how a completion phase of an electronic market for emission permits could be realised. The emission permits are realised as original and anonymous licences. There are some proposals how security and anonymity can be reached in an open network [5]. Besides security and anonymity we have to consider the necessity of controlling the amount of actually emitted toxins in this realisation.

An anonymous original licence - in the following called license - is a digital document, which is an original despite the fact, that there may be many copies. The contents of the licences does not reveal the identity of the owner. Everyone - the owner as well as all former owners - of the license shall be anonymous this way. The proposed system also implements strong anonymity during the buying process, because the buyer's network address is invisible to third parties.

4.1 Cryptographic Mechanisms

For the implementation of original and anonymous licences basic security services are combined in a way, that the properties anonymity and originality are reached. Cryptographic mechanisms are essential to realise these basic security services confidentiality and integrity [16].

Non-repudiation can be achieved by using an additional infrastructure [15]. Both private-key and public-key cryptography is part of our proposal. When using private-key cryptography sender and receiver of a message have to share a key and therefore have to trust each other. With a public-key mechanism, the sender can use the public-key to encrypt, while the receiver is the only person, who knows his private-key, which he uses to decrypt. These two keys of a public-key cryptographic mechanism are inverses of each other. What is encrypted with one can be decrypted with the other and vice versa. Figure 2 shows the symbols which are standing for cryptographic mechanisms in this chapter:

Symbol	Meaning
$e_A(M)$	Encryption of M with A's public-key
$d_A(C)$	Decryption of C with A's private-key
ρ	Generating a random number
$\sigma_A(M)$	Digital signature of A to M
$\upsilon_A(M)$	Verify the digital signature of A to M
$s_K(M)$	Private-key encryption M using key K
$s_K(C)$	Private-key decryption C using K
+	Operator to concat messages

Figure 2. Cryptographic mechanisms

Private-key mechanisms are also called symmetric. Symmetric systems such as IDEA [18] or Triple-DES [21] didn't show vital weaknesses in practical use, although DES has now been used for over 20 years to a large extent. For security a key length of at least 128 bit is recommended at present. Despite the fact, that the Triple-DES has a key length of this order, it is opportune to use IDEA which also uses key length of 128 bit, because it is developed to be fast in software implementation. The RSA [29] algorithm is the standard public-key cryptographic mechanism. Today an RSA encryption is secure, when a key length of minimum 1024 bit is used. RSA can be used for digital signatures, in this case an additional cryptographic hash function like MD5 [28] is used to reduce the message to a fingerprint of constant length. This hash value is encrypted with the secret-key of the signer to obtain the digital signature. Another cryptographic element of the proposed system is a cryptographic random generator, which creates the session-keys [2]. A session-key is used only during one transmission. Among other things it is vital to the system's security, that the randomly generated session-key is not predictable.

4.2 Parties

In this specification of an electronic market for original and anonymous licences a central trusted third party S issues the licences and ensures that only original licences are used and traded [10]. Normally a national or regional authority runs such a trusted third party. At the place of emission of each participant a device E will be installed that will measure the quantity of emitted toxins. In the following we call E the emission place device. Participants have to trust the software and hardware of this device [27]. Therefore it has to be calibrated and sealed by officials.

It is not necessary to trust any other party in the system except S and E. Everyone is protected against fraud and criminal intentions of other participants without making assumptions on the behaviour of other participants. In the following sections we will describe the functionality of the software and hardware, that is installed at the authority S, the emission places E and the participants T.

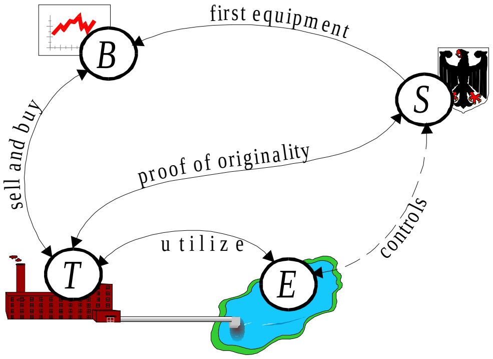

Figure 3. Communication model

In figure 3 the occurring communication flows are shown as arrows between the parties. Between the authority S and the emission place E a dash-lined arrow indicates, that there is no online connection like in all other cases. But sometimes the device at the emission place has to be controlled by officials to discover when a participant has emitted more toxins than the allowed amount.

Everyone can sell and buy licences at the trading centre B. From a technical point of view the trading centre works like a participant T – it buys and sells licences.

4.3 The Emission Permit

In this realisation a *valid emission permit* consists of two parts. The license L represents the permit's subject, while the originality token O_L makes a licence valid, because it guarantees originality of the corresponding license. Originality is realised by the means of being in possession of the originality token and the owner of a licence is able to give proof that he/she is the owner by simply showing the originality token.

Each license L is identifiable due to its serial number n that is assigned consecutively to licences. The licence furthermore contains the description of the environmental quality target U in units per time. The absolute emission quantity per time, that the licence allows to emit, is the percentage u of the total quantity U. In case of a controversy, when the buyer sues for his/her right, the digital signature of the trusted third party S contained in L and O_L is a piece of evidence. The license is valid during a specified period of time: v until b. If this time period runs out, the license loses its validity.

Licence L
Serial number n
Time period v until b
Percentage of environmental quality target u
Environmental quality target U
Digital signature $\sigma_S(n+u+U+ v+b)$

Originality token O_L
Serial number n
Version number t
Digital signature $\sigma_S(n+t)$

Figure 4. Content of a licence

A licence L and a specific originality token O_L, having the same serial number n, belong together. The attributes n, t of all valid originality tokens are stored in the database of the trusted third party. Whenever a token is transferred the trusted third party proofs, if the seller owns the originality token. The trusted third party can do this by comparing the originality token with the corresponding one in its database. There exists always exactly one valid originality token per licence. The participant, who knows the originality token, is the owner of the licence.

A licence L can be copied by everyone, but the originality token was generated by the trusted third party and then transferred confidentially to the owner. The validity of the originality token can be proofed by examining the version number t of the token. It changes every time, when the owner of a licence changes. If two originality tokens contain the same version number, the system treats one as a copy. Therefore, the owner has no profit from illegally copying his originality token, because he would probably have the loss.

4.4 First Allocation

First, the emission permits are given to the trading centre B, where the system's participants T can buy them. The technical realisation allows the buyer to be anonymous - even the network address of the buyer is not visible to the authority. However, when selling the permit the network address of the buyer is visible to the seller. Since we want the first buyer to be able to hide his/her identity from the authority S like the following buyers will be able to, we choose to give the permits first to B. The technical procedure does not restrict the use of economic models for the first allocation such as the Grandfathering. If the Grandfathering is preferred the trusted third party sends the emission permits directly to each participant T.

The emission permit is issued by the national or regional authority. It generates the licence L together with the originality token O_L, encrypts both with the public-key of the trading centre B and sends the result over the unsecure channel of the open network to B. This transmission is confidential due to previous encryption, because only B knows the secret-key to decrypt the emission permit. The trusted third party stores the originality token in its database, because it is needed to prove the originality of the licence during the next transaction, when the trading centre B sells the emission permit. Now, the trading centre offers the emission permits to the public and everyone can buy them anonymously and securely. The trading centre is an electronic marketplace where supply and demand meet.

4.5 Selling an Emission Permit

On selling an emission permit three parties are involved: the trusted third party S, the buyer and the seller. The protocol steps for selling an emission permit are the same, no matter who the seller or the buyer is. It may be two participants T_1 and T_2 or the trading centre B and a participant T. We explain the procedure with B as the seller and T as the buyer.

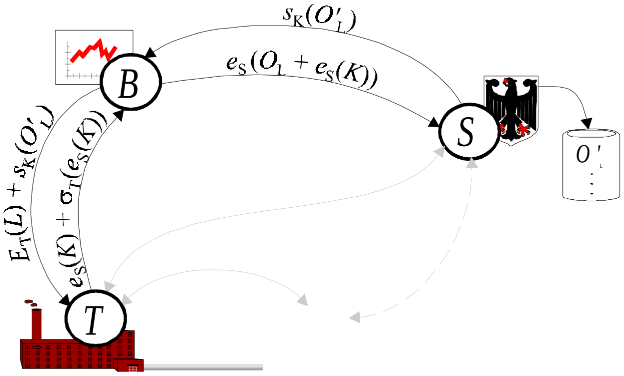

Figure 5. Selling an emission permit

The negotiation between seller and buyer is not subject of this paper and we assume, that there already exists a contract between the seller and the buyer. How the emission permit is transferred form one party B to another party T is showed in figure 5. First, the buyer T generates a symmetric key K with the cryptographic random number generator. Then, he encrypts it with the public-key of the authority S and sends it to the seller B, who receives the message but can't decipher it. Only the authority S can decrypt it to obtain the session-key K, because it is the only one who knows the matching secret-key. A digital signature of *T* has to be attached to the message in order to protect the communication against a man-in-the-middle attack [30].

No.	Party	Content	Description
1	$T \leftrightarrow B$	Price, licence	Contract
2	$T \rightarrow B$	$\sigma_T(e_S(K)) + e_S(K)$	Encrypted and digitally signed session-key.
3	$B \rightarrow S$	If $v_T(e_S(K))$ then $e_S(O_L + e_S(K))$	Check signature. If valid add O_L and encrypt
4	S	$d_S(e_S(O_L + e_S(K))$ Check O_L If O_L valid then $O'_L(n = O_L.n, v = \rho)$	Decrypt Check originality token. If it is valid then generate new originality token with same serial number and a new version number . Store it in the database.
5	$S \rightarrow B$	$s_K(O'_L)$	Originality token encrypted with the symmetric algorithm
6	$B \rightarrow T$	$e_T(L) + s_K(O'_L)$	Licence encrypted (asymmetric) and Originality token encrypted with symmetric key *K*.
7	T	$L = d_T(e_T(\mathrm{L}))$ and $\upsilon_S(L)$ $O'_L = s_K(s_K(O'_L))$ $\upsilon_S(O'_L)$	Decrypt the licence and check digital signature of the authority. Decrypt originality token with the session-key *K* and check the digital signature.

Figure 6. Selling procedure

The trading center *B* has to send the message unchanged together with the originality token to the authority *S*. Since there is the risk that an attacker uses the originality token O_L with a changed session-key *K*, the originality token has to be encrypted with the public-key of the authority *S* during the transmission. After decrypting the message with its secret-key the trusted third party verifies its own digital signature attached to the originality token. So the authority can ensure, that the originality token is not a forgery. Then it searches the serial number *n* in its database and compares the version number *t* of the originality token with the version number in the database. If they are equal, the originality token will be valid and *S* will generate a new originality token O'_L with the same serial number *n*, but with a new version number $t = \rho$. The trusted third party *S* uses the session-key *K* to encrypt the new originality token with a symmetric algorithm and sends it to the seller *B*, who forwards it together with the licence *L* to the buyer. Only the authority *S* and the buyer *T* know the session-key *K*. So nobody is able to steal the originality token. The buyer decrypts the message and obtains the licence *L* and the originality token O'_L. Finally the buyer proofs the digital signature of the authority *S*.

4.6 Using an Emission Permit

Emission of toxins will be only allowed if the emission permit is registered at the emission place *E*. While the emission permit is registered, the owner is not able to sell it, because he does not have the valid originality token. The registration of emission permit is shown in figure 8 and described in figure 7.

	Party	Content	Description
1	$E \rightarrow T$	$\sigma_E(e_S(K)) + \mathrm{e}_S(K)$	Session key encrypted and digitally signed
2	$T \rightarrow S$	If $v_E(e_S(K))$ then $e_S(O_L + e_S(K))$	Check signature. If valid add O_L and encrypt both.
3	S	$d_S(e_S(O_L + e_S(K))$ Check O_L If O_L valid then $O'_L\ (n = O_L.n, v = \rho)$	Decrypt Check originality token. If it is valid then generate new originality token with same serial number and a new version number.
4	$S \rightarrow T$	$s_K(O'_L)$	Originality token encrypted with symmetric algorithm
5	$T \rightarrow E$	$e_E(L) + s_K(O'_L)$	Licence encrypted (asymmetric) and originality token encrypted with symmetric key *K*.
6	E	$L = d_E(e_E(\mathrm{L}))$ and $\upsilon_S(L)$ $O'_L = s_K(s_K(O'_L))$ and $\upsilon_S(O'_L)$	Decrypt the licence and check the digital signature of the authority. Decrypt originality token with the session-key *K* and check the digital signature.
7	E		Record illegal emissions

Figure 7. Registration procedure

After the originality token is handed over to the emission place the amount of allowed emission of new permit is added to the total amount of permitted emission. The registration procedure is necessary because the owner has to loose the licence. Otherwise he could sell it and still emit toxins. On the other hand the emission place device needs to know the licence and how much toxins the owner is allowed to emit. This is very similar to the process of selling a permit since both can be achieved by transferring the valid originality token and the licence from one to another party. The connection to the emission place device is a point-to-point line which is the cheapest solution because normally the emission place *E* would be near to the computer of the participant *T*. Furthermore, if *E* would have an autonomous network connection, it would be able to send information elsewhere. In this case the security would depend on the trustworthiness of emission place device and how robust it is against attacks.

There is no need for a digital signature when sending the message from *T* to *S* (see step 2 in figure 7), because according to our assumption (see section 4.3) nobody except *T* knows the originality token. So *T* is authenticated by only sending the originality token to *S*.

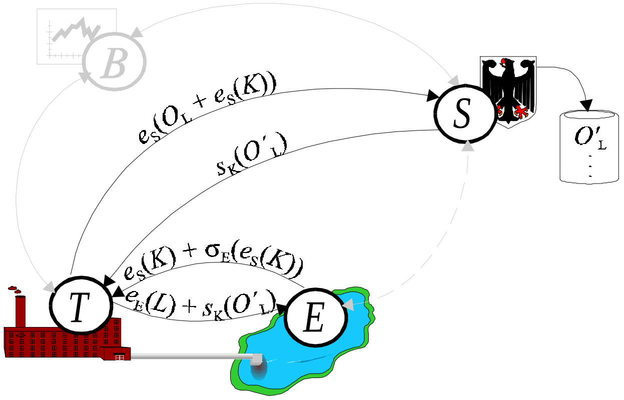

Figure 8. Registration procedure

In the emission place device a integrated measuring instrument measures the actual emission and compares it with the permitted emission. If the participant emits more toxins than he is supposed to, it stores the information about this offence in its memory. The stored information about offences will be evidence to take legal proceedings. Because security seems to be important at this point the following mechanisms have to be integrated in the device:

- Access control to protect the stored data and the measuring instrument against manipulation and unauthorised reading of information about offences.
- Auditing of tried penetration and manipulation.
- Security module to store the private-key of the device in a confidential way.

If the owner want to sell the emission permit he/she needs the originality token. So he/she has to finish the registration period of the emission permit at the emission place device, which sends the originality token back to the owner. For this transmission no trusted third party is required because the emission device itself is a trusted device. The emission place device simply encrypts the originality token for transmission.

5 Organisational Measures

There are some organisational measures that have to be taken to ensure that the system works well and fulfils its purposes. The organisational measures can be classified into three phases by the time they occur. The three phases are the phase of engineering, the phase of installation and the phase of operation. In figure 9 the three phases are given together with their characteristic organisational measures.

The players need to trust the system's hard- and software, that it really works the specified way without doing additional things. That is the reason why producers take security measures during the process of engineering and constructing hard- and software. Furthermore it is preferable to use components with a security certificate according to an evaluation criteria catalogue like the Common Criteria [4]. The software and hardware of the participants and the trading centre are less important to security but the trustworthiness of the technology of the authority and the device at the emission place is vital to the whole system. These parts of the electronic market should reach a high level of certification.

Up to now certifying software- and hardware components has seemed to be very complex and expensive. Software manufacturers try to avoid these costs by giving digital signatures to their products. So they declare themselves responsible for what the software is doing. Although the digital signature is no real substitute for evaluation and certification, it ensures integrity of the product and protects software from becoming infected by a virus and other manipulations.

During the installation phase the authority's computer is installed and starts working. There are two possible threads at this point: manipulation of software and manipulation during the assignment of keys with identities. Checking the trustworthiness of the technicians and restricting their number is one way to prevent against these attacks. The device at the emission place has to be installed and then calibrated. Like the trusted third party, it is supposed to have its own public-key pair. So the keys have to be generated and the device has to be protected during the handing-over. Nobody except the device itself should know the secret-key of this pair of keys. A solution for this problem is that two employees get two different passwords and a SmartCard from the trusted third party, which together enables the device to reconstruct the key. The trusted third party also have to certify the public-key of the key pair. Both, the authority's computer and the emission place device should go on-line after a careful check. The grade, how reliable the system at the authority and the device at the emission place is determines the value of evidence in the case of a legal proceedings. In the Federal Republic of Germany there were examples of judgements concerning Euro-Cheque teller machines, where banks lost against clients because the banks could not prove the system to be secure [23]. While the systems *S* and *E* are running, they need to be protected against unauthorised access. Primarily, this means protection in a very material way. The trusted third party should be located in a secure room, where only a few employees are allowed to enter. Access to data and software through the network connection should be limited to the described protocol actions.

The devices at the emission place need to be robust and secure against mechanical destruction. They should be sealed by officials, in order to spot any manipulation. This way it is possible to punish a saboteur. Data logs of the device need to be checked periodically to detect if the participant emitted too many toxins and authorised access to the log data therefore must be possible for officials. Using a SmartCard with a PIN-number to authenticate a person to the device is a way of achieving a strong access control mechanism. Furthermore opening the device should only be possible with a key. If the device displays an illegal emission, it is able to transmit the data about this illegal emission to a portable computer. This digitally signed data is used as evidence in a legal proceeding.

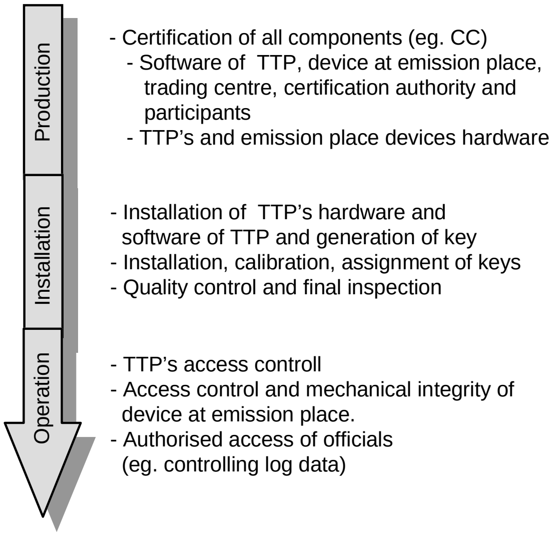
Production
- Certification of all components (eg. CC)
- Software of TTP, device at emission place, trading centre, certification authority and participants
- TTP's and emission place devices hardware
Installation
- Installation of TTP's hardware and software of TTP and generation of key
- Installation, calibration, assignment of keys
- Quality control and final inspection
Operation
- TTP's access controll
- Access control and mechanical integrity of device at emission place.
- Authorised access of officials (eg. controlling log data)

Figure 9. Phases of organisational measures

The general conditions for legal binding of digital signatures in Germany is the Digital Signature Act [3]. It includes certification authorities, which certify public-key. To gain wide-scale acceptance the system should be integrated into the public infrastructure of certification authorities, because otherwise the threshold for a person to participate in the system increases, if he has to handle and take responsibility for yet another key. Each participant can use his/her public-key certified by the public certification authority that he/she also uses for other purposes. Generation and certification of the trusted third parties and the device *E*'s key is the task of the national or regional authority *S*.

6 Conclusion and Further Work

In this work we have specified the completion phase of a secure electronic market for tradable emission permits. The emission permits were realised as original and anonymous digital documents (licences). In principle this concept is applicable to all digital products on electronic markets, that need to be original in order to be valuable whereas other facts plead for anonymity. We have discussed the countermeasures that have to be taken against the risks of an open network like the Internet. Besides the more complex security risks, basic risks in an open network like loss of confidentiality or loss of integrity can be overcome by using cryptographic mechanisms. When selling an emission permit the seller reveals his network address but the buyer is anonymous to a third party. Adding the same anonymity for the seller is in theory possible by using MixNets [25]. Evaluation and certification of hardware and software and its importance was mentioned in this paper. Efficient cheap mechanisms for evaluating information technology products are not yet available.

The inherent transaction costs of trading emission permits are supposed to be lower in this specification of an electronic market than in traditional markets [34]. Lower transaction costs are a big step towards efficiency of tradable emission permits. An other step towards efficiency is the free denomination of the permits.

Its hard to predict the costs of measuring instruments. For some toxins cheap measuring technology is available - but not for others. If cheap technology for measuring emitted toxins is available, then the proposed system is able to provide maximal control with low costs. The devices are measuring emission outputs all the time and staff are only rarely needed. So controlling is with low costs for staff but without a control gap.

From the perspective of the phases of the buying process, we described a secure protocol which realises the completion phase of an electronic market for emission permits. A further aspect of the completion phase is payment. Electronic payment system are able to lower the transaction costs in the completion phase again [24]. Some digital products have to be original others do not. Different digital products need different security services with different strengths. That's why we suppose, that securing electronic markets always depends on the product type. Good example of this are electronic payment systems. Digital cash coins do need to be original, whereas an electronic bank transfer do not.

In our realisation we used the trading centre as intermediary [31], which are called cybermediary in electronic markets. There are any open questions about intermediaries in electronic markets. Concerning our realisation it is still uncertain, if the trading centre is economically the most efficient way for co-ordinating supply and demand.

7 References

[1] Backhaus, K.; Voeth, M.; Bendix, K. B.:*Die Akzeptanz von Multimedia Diensten*. Working Draft 19/1995; Editor: Backhaus, K.; University of Münster; 1995.

[2] Blum, L.; Blum, M.; Schub, M.: *A Simple Unpredictable Pseudo-Random Number Generator*. SIAM J. Computing; 15/2; 1986; p. 364-383.

[3] Beschluß des Bundeskabinetts*: IuKDG Informations- und Kommunikationsdienste Gesetz.* DuD Datenschutz und Datensicherheit 21; Verlag Vieweg; Wiesbaden; 1/1997; http://www.iid.de/rahmen/iukdg_3.html (accessed: Jan. 1997)

[4] *Common Criteria for Information Technology Security Evaluation*. Version 1.0; 1996.
http://www.tno.nl/instit/fel/refs/cc.html#download (Nov. 1996)

[5] Chaum, D.: *Security without Identification: Card Computers to make big Broher Obsolete*. Communications of the ACM; vol. 28; no. 10; Oktober 1985.

[6] Crocker, T. D.: *The Structuring of Atmospheric Pollution Controll Systems*. in: Wolozin, H. (Editor): The Economics of Air Pollution; New York; 1966; p. 61-86.

[7] Dales, J. H.: *Land, Water and Ownership*. In: Canadian Journal of Economics 1; Vol. 1.

[8] Endres, A.: *Umweltökonomie - Eine Einführung*. Darmstadt; 1994; p.6 ff.

[9] Ewringmann, D.; Gawel, E.: *Kompensationen im Imissionschutzrecht: Erfahrungen im Kannenbäcker Land*. Baden-Baden; 1994; p. 38.

[10] Fox, Dirk; Hoster, Patrick; Kraaibeek, Peter: *Grundüberlegungen zu Trust Centern*. In: Horster, P. (Editor): Trust Center; Proceedings der Arbeitskonferenz Trust Center 95; Verlag Vieweg; Braunschweig 1995; p. 1-10.

[11] Gawel, E.; Hansmeyer, K.-H.: *Umweltauflagen.* In: Junkernheinrich, M.; Klemmer, P.; Wagner, G. R. (Editor) Handbuch zur Umweltökonomie; Berlin; 1995.

[12] Gerhard, M.; Röhm, A. W.: *Freier und sicherer elektronischer Handel mit originalen, anonymen Umweltzertifikaten.* In: Tagungsband Verläßliche Informationssysteme VIS '97; DuD Fachberichte; Vieweg Verlag; 1997

[13] Hansen, H. R.: *Klare Sicht am Info-Highway - Geschäfte via Internet & Co.* Ovac-Verlag; 1996.

[14] Huckestein, B.: *Umweltlizenzen - Anwendungsbedingungen einer ökonomisch effizienten Umweltpolitik durch Mengensteuerung*. In: ZfU 1/1993; p. 1-29.

[15] International Organisation for Standardization (ISO): *Information processing systems - Guidelines for the Use and Management of Trusted Third Parties - Part 2: Technical Aspects*. International Standard ISO/IEC Draft 14516-2; Genf; 1995.

[16] International Organisation for Standardization (ISO): *Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture.* International Standard ISO 7498-2 (E); Genf; 1989.

[17] Klein, S.; Langenohl, T.: *Coordination Mechanisms and Systems Architectures in Electronic Market Systems.* In: Schertler, W; Schmid, B.; Tjoa, A M.; Werthner, H. (Eds.) Information and Communications Technologies in Tourism; Wien, New York; Springer; 1994, p. 262-270.

[18] Lai, X.; Massey, J.: *A Proposal for a New Block Encryption Standard.* Advances in Cryptology - Eurocrypt '90; Springer; Berlin; 1991.

[19] Malone, Thomas W.; Yates, Joanne; Benjamin, Robert I.*: Electronic Markets and electronic Hierarchies*. CACM; vol. 30; No. 6; 1987; p.484-497.

[20] van Mark, M.; Gawel, E.; Ewringmann, D.: *Kompensationslösungen im Gewässerschutz;* Umwelt und Ökonomie; vol. 6; Heidelberg; 1992.

[21] National Bureau of Standards (NBS): *Data Encryption Standard (DES).* Federal Information Processing Standards Publication (FIPS-PUB) 46-1; US Department of Commerce; 1/1977.

[22] Needham, Roger M.; Schroeder, Michael D.: *Using Encryption for Authentication in Large Networks of Computers.* Communications of the ACM; vol. 21; no. 12; 1978; p. 993-999.

[23] Oberlandesgericht Hamm: *AZ 31 U 72/96*. Quelle: ARD-Ratgeber Technik; 1996

[24] Pernul, Günther; Röhm, Alexander W.: *Neuer Markt - Neues Geld?* Wirtschaftsinformatik 4/97; Verlag Vieweg; Wiesbaden; 1997.

[25] Pfitzmann, A.; Waidner, M.: *Networks without user observability -- design options.* Eurocrypt '85; LNCS 219; Springer-Verlag; Berlin; 1986; p. 245-253.

[26] Pfitzmann, B.; Waidner, M.; Pfitzmann, A.: *Rechtssicherheit trotz Anonymität in offenen digitalen Systemen (part 1).* Datenschutz und Datensicherheit 5/90; Verlag Vieweg; Wiesbaden; p. 243-253.

[27] Pfitzmann, A.; Pfitzmann, B.; Schunter, M.; Waidner, M.: *Vertrauenswürdiger Entwurf portabler Benutzerendgeräte und Sicherheitsmodule.* In: Brüggemann, H.-H.; Gerhardt, W. (Editor): Proceedings der Fachtagung Verläßliche IT-Systeme VIS '95; DuD-Fachberichte; Verlag Vieweg; Braunschweig 1995; p. 329-350.

[28] Rivest, Ronald L.: *The MD5 Message-Digest Algorithm*. Request for Comments (RFC) 1321; Network Working Group; 4/1992; S. 1-21.

[29] Rivest, Ronald L.; Shamir, Adi; Adleman, Leonard: *A Method for obtaining Digital Signatures and Public-key Cryptosystems*. Communications of the ACM; vol. 21; no. 2; 1978; p. 120-126.

[30] Rivest, Ronald L.: *How to expose an eavesdropper*. Communications of the ACM; vol. 27; no. 4; 1984; p. 393-395.

[31] Sarkar, M.; Butler, B.; Steinfeld, C.: *Intermediaries an Cbermediaries: A Continuing Role for Mediating Players in the Electronic Marketplace*. JCMC; vol. 1; no. 3; 1995; http://jcmc.huji.ac.il/vol1/issue3 (accessed: Nov. 1996)

[32] Schmid, Beat: Elektronische Märkte. Wirtschaftsinformatik 35 6/93; Vieweg-Verlag, Wiesbaden; 1996.

[33] Weiler, R.M.: *Money, transactions, and trade on the Internet*. MBA thesis; Imperial College London; 1995; http://graph.ms.ic.ac.uk/results (accessed: Jun. 1996)

[34] Wigand, R. T.: *Electronic Commerce and Reduced Transaction Costs.* In: Alt, R.; Zbornik, S. (Editor) EM - Electronic Markets; no. 16/17; vol. 5; St. Gallen; 1995.