Dear valuated reader of the Emission News!
As we have announced since October 2014, the Emission Newsletter will be a paid subscription service from March 2015 onwards.
The present issue is only partial readable, as it remains free of charge.
Information about the paid version and on how to subscribe to the full version of the newsletter can be found here and on www.emissionshaendler.com

Emission News 11-2015

Practical Information for Emission Trading
Edition 26.10.2015

EUA DEC15 01.01.2015 to 23.10.2015 Source: ICE London

Cybercrime in Online Banking Could Harm Safety of Union Register - 3 Years Updates Occurring

Incorrect activities of authorized representatives in the register might cause the possibility of a certificate theft in case of an insufficiently secured mTAN procedure. Due to fraud series with stolen mobile TAN numbers (mTAN) in online banking leaked out lately the question arises in how far certificates of the Union register's account are still safe if simultaneously authorized representatives of a system operator violate the register regulation's rules. Emissionshändler.com® examines in its Emission News 11-2015 being presented here the possibilities and procedures leading probably to a possibly successful cyber theft of certificates (as already happened in 2010).
We furthermore report about the running invitations of DEHSt to update data being necessary for the opening (at that time) of an investment account of the system operator as well as about personal data of the relevant authorized representatives. We also reproduce in a foreign reporting from BBH a survey about the level of the financial market directive MiFID II and how this would impact on system operators, traders and public utilities.

New Certificates' Theft of Register Accounts probably only a Matter of Time

According to latest news about security gaps in the TAN procedure, certificates' theft of CO2 register accounts seem no longer be impossible.

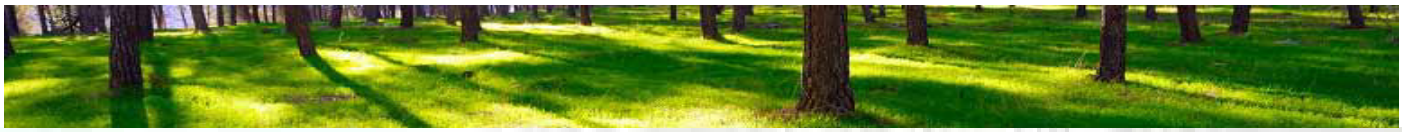
This is the case if the authorized representatives of the register account do not or only incompletely

A possible loss may be many times higher than those of cyber thefts of up to 30,000 Euros being launched lately and having to be borne by Telekom customers.
The reason why all victims obtained a compensation so far may be that they are not to be blamed for the loss in most cases or acted negligently only once by

According to Emissionshändler.com®'s judgement, a compensation of loss due to Phishing in a certificates account would be almost impossible because in case of a cyber theft, an authorized person would also carry out an intentional offence against the register regulations' rules. This is often the case, according to Emissionshändler.com®'s experience, which means that it will only be a matter of time until corresponding on register accounts will take place for will personally be held responsible.

The mTAN Procedure shows Security Gaps

Within the last weeks a phishing series took place in the German Several media reported about a lot of defrauders who deducted five-figure sums from concerned, the total loss amounts to more than a million Euros so far.



The 2-channel authentication method with PC and mobile device (being also used for the CO2 Union register) has been classified as safe until now because the mTAN generated by a system enters over the mobile device thus being independent from a PC which might be infected with a Trojan.
The mTAN system had been working almost trouble-free for nearly 5 years but now criminal professionals are acting with high criminal energy and technical know-how. Customers [illegible] are concerned so far. It is said that they only had cell phone contracts with Telekom and were working with the mTAN system.

The Defrauders' Method Takes Place in Several Steps

First of all a Trojan (spyware) entered into the victim's computer. There the access to the online account together with the appropriate password was searched. Already here or on other ways the victim's cell phone number has been found as well as possible customer pass words probably needed for the authentication at the provider. Then the defrauders [illegible] of a [illegible] towards Telekom and asked to unlock a blank SIM card in the name of the customer, this for an allegedly lost card (blank SIM cards are physically always available in shops) respectively asked to send a SIM replacement card to the "shop's address".
As soon as the blank card is unlocked respectively the replacement card with the customer's phone number is in their hands, they carry out [illegible] the victim doesn't notice in time or only later. This is a way to practice the method of a double SIM card. The offender uses a so-called multi SIM card for this process which means a card that can exclusively receive SMS under the same cell phone number without being obliged to turn off the previous SIM card. For the victim everything seems to be okay, he/she can telephone without problems, probably no SMS arrive for several minutes [illegible]
However, if the offender decides for the method of a usual SIM replacement card, the victim may notice irregularities much earlier because his/her SIM card does [illegible] as soon as the offender has put it into his cell phone. [illegible] neither will he/she receive phone calls or SMS.

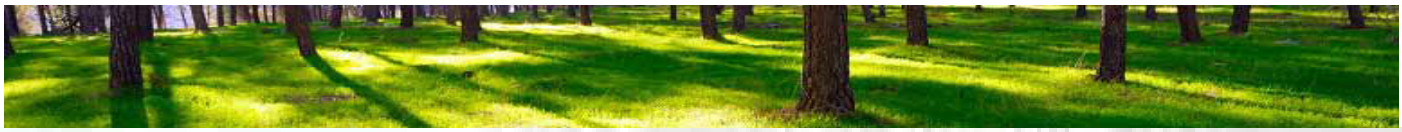
Present Countermeasures and Further Methods of the Defrauders

We found out in the meantime that Telekom took measures against the SIM card issuing and identification of traders and shop owners in order [illegible] Especially the provision of blank cards to shop owners and the sending of cards to customers by [illegible] postbox could be of interest for the defrauders.
We can assume that also other mobile phone providers are affected by "invented shop identities". Even if this is not the case and other providers of this business line would protect themselves by similar safety measures, criminal gangs will [illegible] by the mTAN procedure.
Already in 2014 it became known that smartphones being infected with the Android Trojan Fake Token can be treated in a way to pick off mTANs, enabling the criminals to empty the cell phone owner's account.
It was published on 24th October 2015 that according to a message of the Heise Security Portal, research workers of the Erlangen University succeeded in breaking into the mTAN-App of [illegible] (savings bank), redirecting amounts of money and to modify its sums as desired.

Infobox:
Taking over of invalid/ineligible remaining stocks of CER/ERU

*Emissionshändler.com® offers all investment operators **and Airlines** to take over all their remaining stocks of invalid CER/ERU before they can no longer be transferred from 11.18.2015.*
*Emissionshändler.com® pays 0,5 EuroCent/t, 250.00 Euro max. to each investor, a total of 1.00 Euro minimum at least, however, for taking over **invalid**/ineligible CER/ERU.*
*The seller receives in any case a Word template as a file, enabling him to present an invoice to Emissionshändler.com® of **1.00 Euro minimum**.*
*If the account holder needs help to set up a **trust account** for Emissionshändler.com®, free assistance and solutions will be offered.*

Caution: Setting up a trust account is no later than 11.5.2015 necessary
For the request of a selling form, interested investment operators address themselves to Emissionshändler.com® under info@emissionshaendler.com



Cyber Theft of Certificates (Now) Became Possible Again

While considering the criminal activities around the mTAN procedure known until now, the future theft of CO2 certificates in the union register becomes more and more likely.

In this context we have to repeat that the Phishing attacks beginning of 2010 in various different national CO2 registers were [illegible] The today's union register with the pre-connected ECAS authentication system presents a sufficient safety standard. However, this is only the case if the 2 channel procedure and the 4 eyes principle are respected completely and correctly.

Basing on the fact that it is no longer impossible to that actions and influence are taken on the mTAN procedure by criminal defrauders, account holders and authorized persons should draw their attention to their existing security structure and their internal workflow process.

How a Cyber Theft of Certificates Could Take Place in a Union Register?

The reason for future successful attacks might be found especially in the following ways of action practiced by authorized register account owners:

a) The authorized representative A is alone in the office and uses the access and the service cell phone of the second authorized representative B (with his approval)
b) The authorized representative A is alone in the office, authorized representative B is ill or left the company. A uses the access and the service cell phone of authorized representative B with or without his approval
c) The authorized representatives A and B use [illegible]
d) The authorized representatives A and B [illegible]

Basing on the fact that [illegible] is infected with malware, it would be possible according to nowadays knowledge that an unjustified transaction by a criminal defrauder will be generated.

The consequence of cases [illegible] would be that the second authorized representative asked the [illegible] what the [illegible] which he has to confirm. The [illegible] that one of both PCs might be infected and the second authorized representative's smartphone transmits mTANs without permission would already generate a confirmed transaction.

If we consider the above-mentioned points [illegible], however, this incorrect activity might lead to the fact that by means of repealing the 4 eyes principle a confirmed transaction being generated by unauthorized third parties can be started. As the authorized representatives will not receive an SMS on their cell phone, the only chance for a reaction in time [illegible] sent within the 26 hours transaction delay.

Conclusion on the Safety of mTAN in the Union Register

It is a matter of fact that the risk and the potential damage in case of mTAN abuse in the CO2 register can be considerably higher than a Phishing action in the online banking process. This especially because there are no upper limits for certificates transactions and because a transaction carried out once is irrevocable. On the contrary, however, the likelihood of a successful certificate theft [illegible]

Infobox

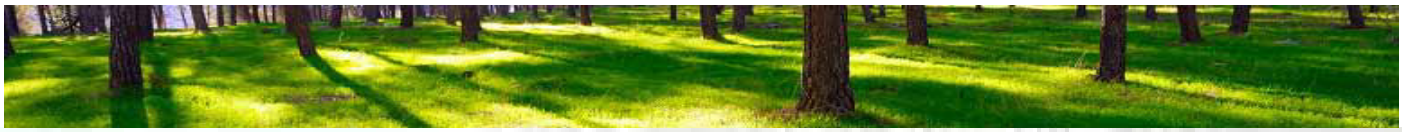
The account package minimizes legal risks

The CO2-account-package from Emissions-händler.com® frees the company largely of high risks, which can occur because of improper accounting or because of a technical or human error.

The establishment of an external account representative by Emissionshändler.com® who also supervises the administrative and legal appointments of the company as well compensate the failure of authorized representative (BV) and / or their actions through the often-updated registry software support.

Detailed information about CO2-account-package can be found on https://www.emissionshaendler.com/en/home.html, via a free telephone line in Germany 800-59060002 or by email info@emississionshaendler.com.

But if certain activities will spread, like ignoring intentionally article 34 (1) items a) to c) and the abrogation of the 4 eyes principle by means of an unjustified access to the register and/or by means of



an identity abuse, an operator has no right to complain an occurred damage. The fact that the operator is entitled to announce liability claims against his authorized representatives will hardly bring him any financial advantage.
It seems much more useful in this context to minimize the risk in advance by choosing for example an external service provider for one of the authorized representatives. Moreover, accesses to different mobile phone providers should be used (see also info box page above).

==========

Updates Not Announced in Time can be punished with Blocking of Authorized Representatives and Register Accounts

As most system operators know, the new register regulation 389/2013 came into effect on 2nd May, 2013. This regulation replaced essential parts of the former regulation and ruled substantially the purposes of the union register being introduced already a year before in June 2012. The latter replaced the national registers. One of the most important contents of the regulation expresses here the topicality of all statements.
Most of the system operators disposed already of a national operational account at the time of introduction of the new union register in June 2012 which was The only requirement was that the mobile cell phone number of an authorized representative was supposed to be Now since July 2015 at the latest, one of the most essential rules of the regulation 389 becomes effective. This is article 25 (4) mandates the register authorities to check many statements around the register account within a 3 years' time limit.
Beside the **topicality** already mentioned, also rules for the **completeness**, the **correctness** as well as for the **exactness** of the appropriate data are meant. The following data and statements will be verified:

- the system
- the responsible of the system
- the
- the

In individual cases the national register authorities might have respected this 3 years delay for a few operators, but most of the account holders and authorized representatives of the German Register receive a corresponding invitation by the DEHSt only since summer 2015 - which is beyond the 3 years review period. One or another legal specialist might be kept occupied by isolated cases in the late future, if a system operator would ever enforce a damage being caused by a verification not being executed by the authorities within the prescribed period – no matter how constructed such a damage would ever be presented. In any case it seems to be usual, like scattered updates within the 3 years delay in conformity with article 25 (4) initialized by account holders and authorized representatives. The reason for their reservation is that they feel disturbed which is a systematic query of data.
In this context a system operator and his authorized representative have the choice either to renounce of a 3 years delay which requires the admittance of certificated personal papers, certificates of good conduct, commercial register extract, etc. to the authorities or to act to carry out the update.

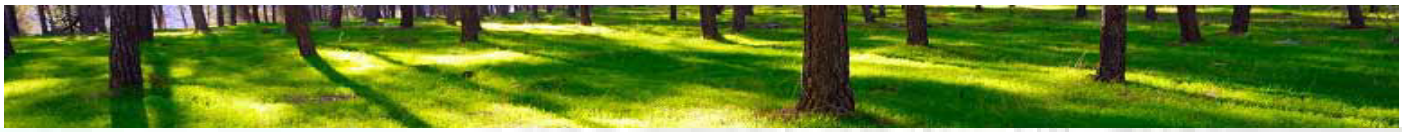
Which Data Will be Verified at least One Time Within 3 Years

The Commercial Register Extract

Account holders used to be required by mail to present an updated commercial register showing its contract rules and the persons being authorized representatives. Normally an electronic summary of the relevant District Court is sufficient. The commercial register extract must not be older than 3 months.

The Certificate of Good Conduct

An updated certificate of good conduct of the account representatives not being older than 3 months has to be presented every 3 years. A certificate of good conduct is preferred in this case because it is the issuing authorities to the
If the authorized person should have the national register authority requires in many cases a separately certified certificate of good conduct which additionally will have to be translated with a



The ID Card or Passport

As national identity documents and passports use to expire after 10 years, the holders will receive another ID or passport number together with their new identity documents. Only for this reason the national register authority is obliged to supervise the relevance of the indications within a 3 years delay, this in accordance with regulation 389 attachment VIII in connection with article 25 (4). The authorized person will be required to present a new identity document. The identity document must include at least - beside the name, first name, place of birth, date of birth - probably proven additionally

It remains to be said that the kind of transmission (electronically or by paper) and the safety standard (certified or uncertified) according to regulation 389 is often left at the discretion of the national authority. In individual cases the authority can insist on an authentication of a or a notary.

The To Dos Of the Account Representative

After an account representative is contacted in a rotation of a 3 years delay by mail by his registration Authority and has procured all required documents, he will have to send them to by VPS

When the Registration Authority has checked the documents and has sent a confirmation by mail that the verification turned out to be satisfactory, the account representative is requested to update his personal data, especially the kind of the identity document ID card or passport and its ID number. From the view of the account representative this is not really logic if he just has transmitted these data to the authority. But it must be known in this context that the update of the identity data but on the representative's URID number. Only the account representative has access to this field. If the account representative will not realize these updates within an adequate period of time, the authorities will first demand banned from the account access

Special To Dos For the Account Holder

As the Union Register is working since June 2012 and also a complete 3 years delay for the "verification of data for an account opening" has passed, account holders are recommended to consider article 25 (1) as especially serious. This article prescribes them to inform within 10 days about any modification of data and information about the attachment and its contact persons which might have changed.

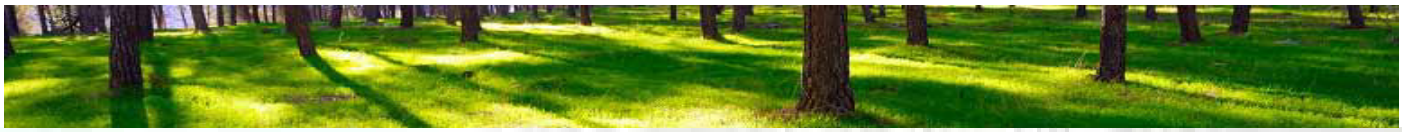
It can be seen from attachment VI-I and attachment VI-II what kind of data might be concerned by this prescription. All in all 32 possible data can be meant from which This could practically mean that for example an information about a can lead to an account lockout with all further consequences.

==========

By courtesy of the Attorneys Becker Büttner Held we are permitted to reproduce the following summary of the office's energy trade newsletter dated 14th October, 2015.

MIFID I and II - Developments, Situation and View

While the practical implementation of REMIT is the present application theme in many houses, the development of the financial market regulation is pursued with the same excitement, especially the amended financial market directive (MiFID II) as it bears the decision whether complete business types could be applied in the future.



In fact the MiFID was brought on the way last year but the national realization is still to be made. And on European level discussions are lead about commodity derivatives (point I.) and the interpretation of secondary activity exception (point II), the definition of both items being decisive for the energy trade.

I. The Derivatives Definition

One of the financial market guideline's central points is the line-up of financial instruments being listed in attachment I section C. In this context it is important to consider that not only the definition of (commodity) derivatives with relation to MiFID II is concerned but also with relation to MiFID I.

1. Commodity Derivatives in Accordance with MIFID I

Beginning of May 2015, the European supervisory authority ESMA published guidelines for the definition of commodity derivatives under C6 and C7. Reason for this guideline is the guarantee of a unified and consistent definition and application in order to achieve a unified definition with the EMIR - this after approximatively eleven years of MiFID publishing! Remember: we talk about a commodity derivative if a forward transaction is concerned and if it is either made on a stock exchange market or via a so-called trading platform (MTF - Multilateral Trading Facility) or if it is realizable (which means that instead of the delivery also a financial compensation is contractually planned). Conversely this is why physical OTC trade deliveries are constantly without supervision because they are not representing financial instruments.

But it was not quite clear to understand what is meant with a "physically settled" business. ESMA's guidelines include an explanation. ESMA confirmed that Forwards being concluded on a regulated market or by means of an MTF belong to the application of MiFID I. Besides, ESMA pointed out that a "physically settled" transaction is made as long as

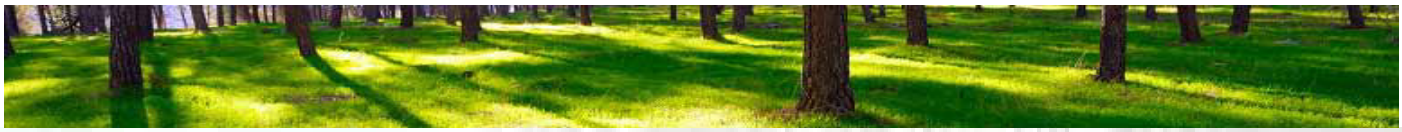
- a real physical delivery has been executed
- the ownership has been transferred by means of an appropriate document (for example delivery note, warehouse receipt) or
- another ownership transfer has been carried out even without physical delivery, classically these are schedule transactions.

2. Commodity Derivatives in Accordance with MIFID II

MiFID I is concerned but not MiFID II. The latter provides that corresponding delegated acts-in-law of the commission are supposed to be offered. To prepare this act-in-law ESMA lately published a Technical Advice which is a legislative assistance for the commission. ESMA is supposed to define expressively for energy wholesale products the term "physically settled" - and ESMA advances one step further than in its MiFID paper: Their proposal provides that the "physical settling" is supposed to depend, among others, on so-called "proportionate arrangements" of the trading partners for production respectively consumption. This is of considerable importance for trading partners who want to refer to a physical delivery because they are obliged to take care that the physical delivery fits with their (industrial) activities, their products, their store capacities respectively their rate of consumption. If this condition would be interpreted disadvantageously, a consequence will be that for example an energy supply company was allowed to buy only as little as it is capable to supply to its customers respectively sell only as much on the wholesale market as it is capable to produce.

This subject is so explosive for power companies because the (sector specific) simplification of the derivatives definition depends on it. As you know, according to MiFID II also the so-called organized trading platforms (OTF), which mean also the smaller broker platforms, are supposed to be covered by the duty of supervision. This means that every forward transaction being made by OTF will be considered as a derivative and will become a financial instrument being due to be supervised. An exception has finally been accepted for the energy sector: expressively REMIT transactions are excluded from the OTF extension but only if they are exclusively realizable physically.

Besides: ESMA now primarily announced how many derivatives are used in Europe actually as the Trade Repositories who accept EMIR messages are requested to publish aggregated data with regard to open items, the transaction volumes as well as values of each derivative class. As a result, more than 16 billion data transfers took place since reporting obligation in February 2012 which means approx. 300 million per week, evaluated 29th May 2015. The data assorted in accordance with the



rough asset classes can be viewed on the websites of Trade Repositories. The figures refer to all commodity derivatives and not only to energy (or even electricity or gas).

II Secondary Activity Exception

As you know, the MiFID II world will no longer include the today's secondary activity exception being applied by most enterprises of the energy sector. The exception will be limited in the future. It will not be possible to apply it for the execution of client orders. In fact contemplation cause 25 of Mi-FID II provides the non-application of this restriction if it is an outside activity for both partners. But after all it will be important to see how this basic idea will be integrated into the national right. The question how main and secondary activity have to be delimited from each other is supposed to be drawn up by the European Authority ESMA Regulatory Technical Standards. ESMA published a proposal on this subject end of December 2014 and again in spring 2015, inviting for a consultation. While ESMA proposed in the beginning to talk about a secondary activity if this would mean "less than 50%" of the main activity, the threshold was reduced to "5%" by ESMA. This step was followed by displeasure and uncertainty among the enterprises who feared to suffer from this regulation. When ESMA heard from these doubts, they announced on the occasion of a hearing in the European Parliament in June 2015 that essential improvements of the ESMA proposal regarding the secondary activity exception can be anticipated. Meanwhile the improvements can be read in a draft dated 28th September 2015. According to this draft a two-step test is planned: First of all the whole market has to be considered which means the enterprise's activities will be compared with the activities of the whole market. The second step includes a test at group level which means the trade intensity respectively the "speculation intensity" of the enterprise. The question whether a secondary activity is still practised will be answered as follows in short words: The more activities an enterprise can show, the smaller its market share may be.
This means first of all: Enterprises are requested to check on a group basis to what extent activities are practised not being applied for hedging reasons, in proportion to the total derivatives share. Depending on the extent of these activities, the consequences will be seen on the threshold of the first test. As soon as the activity exceeds 10%, the threshold level will be halve of the first test. In case of activities over 50%, the enterprise's activity must be lower than 1/5 of the first test's threshold level.
The value thus determined lies in proportion to the market activity where the enterprises can summarize the total of their derivatives but put aside their hedging transactions. Every asset-class hat its own threshold: EL is at 6% and gas at 3%.
The above-mentioned values are not yet carved in stone: The commission has 3 months' time to check ESMA's proposals. Afterwards the European Parliament and the Council will take part in the negotiations. We may follow them with curiosity.

Disclaimer

This Emission News is issued by the emission GEMB mbH and is for information only. The GEMB mbH is neither legal nor tax advice. If this impression, it is hereby clarified that this is neither intended nor desired. The GEMB mbH assumes no responsibility for the accuracy and completeness of the information or its suitability for a particular purpose, either express or implied, this Emission News is not written with the intention that readers make an investment decision, a purchase or sale decision regarding a CO2 product or market and / or a contract decisions in all other respects active. All price curves shown here are based on data from the ICE London, generated from a Reuters information system.

Our offer

Please contact us without obligation at +49 (0)30-398 8721-10 or info@emissionshaendler.com as well as via mail or find out more about the Internet services under www.emissionshaendler.com.

Kind emission regards

Michael Kroehnert

Responsible for content:
Emissionshändler.com®
GEMB mbH, Helmholtzstraße 2-9, 10587 Berlin
HRB 101917 Amtsgericht Berlin Charlottenburg
USt-ID-Nr. DE 249072517
Phone: +49 (0)30-398872110, Fax: +49 (0)30-398872129
Web:www.emissionshaendler.com Mail:info@emissionshaendler.com