Opinion/Statement
on the

Proposal for a
Regulation of the European Parliament
and of the Council
on the Electronic Identification and Trust
Services for electronic transactions in the
internal market,

drafted by the European Commission
in Brussels, 4.6.2012
COM(2012) 238 final
2012/0146 (COD)

Version of this Opinion/Statement document dated: **15th Oct 2012**

Proofread/Edited on 11th December, 2012

Author: Mgr. Ing. **Vojtěch KMENT**
AXONNET, spol. s r.o.

Document created for:
+
Ministry of the interior (of Czech Republic)
European Commission

DISCLAIMER

This document is provided "AS IS". No Warranty on the correctness of the contained information is provided. Readers of this document use the information contained at their own risk.

ABOUT THE AUTHOR

Vojtech Kment integrates the qualifications of computer engineer and lawyer within his own skill set.

He studied the matter of e-signatures extensively over the last 10 years. Among other activities, he is the author of *"Electronic signature in Czech Republic (2006)"* (http://www.epodpis.info/, CS), which covers cryptography, law, IT implementation and a wide variety of related standardization in this field. The report further includes the existing EU electronic signature legal framework and related technical standards created by the European standardization bodies. The report was aimed at the implementers and users of e-signatures within large organizations and companies and is 550+ pages long.

Mr. Kment also participated in deploying e-signature technology in very large organizations. He is also the author of the methodology; "E-signature deployment within larger organizations, 2011, CS".

He has 17+ years experience in the computer security area.

Over the years, Kment developed the multicriterial maxim for e-signature deployment, which is expressed in the paper *An Electronic Signature Maxim, 2012* (http://courttechbulletin.blogspot.cz/2012/05/electronic-signature-maxim.html, EN).

CONTENT

INTRODUCTION

This document contains the independent’s consultant opinion on the *Proposal for a Regulation of the European Parliament and of the Council on the electronic identification and trust services for electronic transactions in the internal market,* drafted by European Commission in Brussels, 4.6.2012 COM(2012) 238 final, 2012/0146 (COD) /further only Proposal/.

This opinion does not represent the interest of any particular technology, service provider or manufacturer.

If this opinion favors any party, it is the natural person who is designated as **signatory** and/or **relying party**.

This opinion/statement is written *pro bono*, ie. without remuneration from any party.

The text of this opinion is divided into chapters (heading level 1). Each chapter concentrates on comments that are similar in nature from certain points of view.

Individual comments are contained within the individual paragraphs (heading level 2). Each paragraph represents a comment on one issue. When the comment is related to other comments, the reference is provided.

Each comment heading contains an indication of its seriousness. This is indicated by "*" characters written within parentheses. One star indicates the least severe issues, five stars the most severe.

The language style of this document aims to mainly expose those conceptual issues relating to electronic signature that arise from the Proposal, when its text is interpreted by knowledgeable IT and legal experts. The aim is to make clear is the nature of the problem, what may be the goal and which intended outcomes are preferred. At the moment, this document does not suggest exact legal or technical wording. At most, it pinpoints wording within the Proposal that is, for some reason, considered unsuitable.

This opinion concentrates on issues related to electronic signatures and is less concerned with electronic identification.

Because of the lack of the time (only 4 days to analyze the Proposal and write this document), this opinion may miss some important issues.

This opinion was created very quickly and further re-evaluation of the expressed comments would normally be performed by the author.

References used, like Art. 7 (3) ..., Recital 15 etc. always refer to the document of the Proposal.

References prefixed Cf. refer to other paragraphs of this opinion.

Abbreviations

CSP - Certificate Service Provider, in the Proposal it is (qualified) trust service provider

SCD - Signature creation data, commonly private key

TSP - Trust service provider

QTSP - Qualified trust service provider

I. Critical objections

Unsolved critical objections would entail serious problems for the electronic signature framework.

I.1 Public bodies as the certified subject within the qualified certificate for electronic seals (*****)

The Proposal expects that electronic seals are created only by legal persons /eg. Art 19 (1)/. However, according to the laws of Czech Republic, public authorities are not usually considered legal persons. Far more often they are considered to be the *organizational parts of the state*. Even municipalities may have offices or bodies that may constitute separate organizational entities having certain features of independent legal subjects (entitlements, obligations, competencies, management ...) and communicate under their own names, yet do not constitute a legal person (own property). Such public bodies very often appear in the qualified (system) certificates within the Czech Republic!

Recommendation: The Regulation should add the following category of subjects: ***public body*** besides the *legal person,* whenever the occurrence of *legal person* takes place and the public bodies are intentionally not aimed to be excluded from the occurrence. Any similar term might be used (eg. *public authority body*). Above all, the *public bodies* should be included as the possibility of the subject that may be certified and whose name is included in the qualified certificate for electronic seals.

I.2 Missing regulation on the employee – employer relationship (****)

Many qualification certificates fail to be requested and issued, not because of the interest of the signatory (a natural person), but because of the interest of the employer. Such certificates usually also contain the name of the employer and the role or function of the employee in his organization. This is especially in the event of an employment termination as the employer must be entitled against the CSP to revoke the issued (qualified) certificate without the consent or any action on the part of the formerly certified employee.

From the point of view of the protection of the employee, he or she should be able to select within the qualification certificate the constraint, clearly available to any third party from the content of the certificate itself, that it may only be used for intra-employer relations and/or for the representation of the employer to 3rd parties. That means it cannot be used for the private relations and other transactions by the employee itself. This protects the employee in cases where the employer deploys relatively weak products from the damage that might happen to him privately. Thus far, qualified certificates issued to the employees are not legally restricted in any way. The objection that the current manner allows wider proliferation of e-signatures should be weighed against the fact that employees are normally at the mercy of their employers. The employer is normally the owner and administrator of all PC components, software, smart cards, phones ... etc.

Recommendation 1: In the case where qualified certificates for electronic signature (for electronic seals, if seals are extended to be issued to natural persons too) is issued because of the primary interest of the employer, whose name is also attached to the above mentioned certificate, this employer is entitled to revoke the certificate independently of the certified natural person.

Recommendation 2: In cases when the qualified certificate for the electronic signature (for electronic seals, if seals are extended to be issued to natural persons too) is issued because of the primary interest of the employer, whose name is also indicated in the above mentioned certificate, the employee is entitled to constrain the use of the above mentioned certificate for intra-employer relations and/or for the outside representation of the employer to 3rd parties and exclude any other use of such certificate. The constraint must clearly be included in the above mentioned certificate.

I.3 Responsibilities of the signatory (****)

The Proposal does not state any responsibilities of the signatory. Perhaps some responsibilities may be implied, but this diminishes the legal certainty. Common responsibilities are the protection of SCD and of the qualified signature creation device, along with the prompt reporting of every security incident to the CSP.

One of many other examples of responsibilities of signatory is the answer on this question: *"may the signatory lend his qualified signature creation device to any 3rd person in order to perform certain tasks, including. electronic signature creation on the behalf of the signatory?"* It is not possible to imply a yes/no answer from the wording of Art. 3 (7) (c), because "can" is not equal to "has" and nothing else may be certainly implied either.

If the answer is yes and the 3rd person oversteps its mandate, does the signatory remain the legally responsible person for the relying party? If the answer is no, and despite it the signatory lends its qualified signature creation device to any 3rd person in order to perform certain tasks on behalf of the signatory and does not exceed its mandate, however it is later realized that the electronic signature was created in this forbidden manner, does the electronic signature still remain legally valid? Is the good faith of the relying party protected or is the signatory more protected?

Recommendation: formulate the major responsibilities of the signatory.

I.4 Responsibilities of the relying party (***)

The Proposal does not provide any list of responsibilities of the signatory. Some responsibilities of the relying party may perhaps be implied, however in this regard the legal certainty is low. A common responsibility of the relying party is to verify the e-signature validity in a proper manner.

Recommendation: formulate the major responsibilities of the relying party.

I.5 Clearly resolve all cases of possible damage (****)

The electronic signature framework is, unfortunately, a case where each participating party may be entirely honest and fulfill all its legal obligations, yet a successful attack against the relying party may occur. Eg. the attacker may crack the cryptography algorithm or, more likely, its implementation in any product or system. Even under these circumstances it must be clear who bears the liability for damage to the signatory-relying party.

Recommendation: clearly resolve all cases of possible damage.

I.6 Transition period at least 2 years (***)

The regulation Proposal assumes entry into force on the 12th day after its publication in the *Official Journal of the European Union*. This is a very unfortunate legal practice that technical practice cannot catch at all. The regulation should postpone its entry into force for at least two years.

Only propositions empowering the European Commission to issue their implementing or delegating acts should be immediately entered into force.

Recommendation: postpone the entry into force 2-3 years, except for the empowering provisions.

I.7 All delegating and implementing acts to be issued at least 1 year before the regulation's final entry into force (***)

Many details are deferred to implementing or delegating acts. This is a proper legislative technique. Yet these details are crucial. It is necessary:

- to have a review process of the text of these acts prior tp official publication; that should also include the technical standards assumed to be obligatory by these acts, eg. 1-2 years,

- to have sufficient time to allow the implementation of the acts, eg. 1 year.

Recommendation: prepare and allow the review of all acts and standards prior to their official issue and provide a sufficiently long period for their implementation.

II. Conceptual matters

II.1 Authentication – Identification

Computer security literature provides no single and exclusively accepted definition of the term *authentication*. Very often the definition is similar to: ***Authentication*** *is the process verifying the claimed identity of the subject*. In this way, any difference between the terms ***identification*** and ***authentication*** may disappear and become easily confused! I suggest great care when these two words are used in the Proposal, in order to avoid any such confusion, as well as more exact definition in circles, tautologies etc.

Even authentication defined as cited above is considered to include some evidence proving or disproving the claimed identity. I.e. *authentication* must include some kind of technique or technology and this is at the heart of its meaning.

Some ISO standards defined authentication a bit differently. Basically, ***authentication*** *is a method by which the communicating entities verify "who" is the opposite entity*. Some of these entities could be human beings, however very often it is the case that purely technical entities (software or hardware) mutually communicate. This definition seems similar to the first, however instead of *identity* it shows only the more vague *"who"*.

Let us explain it by example. Some file server may use the login/password authentication. Let us name that user John Newman. The authentication is initialized by somebody so that the login name is set to "John" and its password to "Abr32aka3". From that moment Mr. John Newman may login to the file server using those credentials. At the beginning of the session the file server authenticates the user and concludes that it is "John". John is thereby approved to access certain folders. It should be clear however, that this file server knows nothing special about John. It does not know that his full name is John Newman, nor whether the name John is a real name, a pseudonym or a false name. It does not know the John’s date of birth or his home address.

Authentication may also occur between only technical entities. Imagine that a mobile phone and desktop PC have been configured for mutual communication using the Bluetooth protocol. After initialization, they may synchronize certain data, eg. the personal calendar present on both devices. However they may only recognize each other as "Nicenotebook" and "Myfavoritephone". These two devices need not know the actual user of each device.

Authentication is about "sameness" or certain attributes of the opposite entity and the method/process by which these sameness attributes are proved to belong to the opposing entity. **Identification** is about "identity" in the common human sense of identity.

Identification *always* involves some authentication technique, however it does not *necessarily* involves identification.

These days there are basically only two methods of remote electronic communication:

1. **On-line interactive session.**
2. **Communication via off-line message.**

The typical current example of the **first** method is the session between the web browser user and the remote web server application.

The typical current example of the **second** method is the creation of an electronically signed document by the user, which is then sent to the opposite party.

It should be understood that both methods usually require ***authentication*** of the user and that both methods may require the ***identification*** of the user. Of course the methods of authentication and identification differ significantly among these two methods.

However, the situation is not that identification or authentication only plays a role in the first method. In fact, the electronic signature is mainly an authentication of the origin of the message. The identification requirement may be added as well.

The first method is the typical method by which computers work and have been used since their invention until today! Only the communication link is more complex and more remote than it previously was.

On the contrary, the second method is rather artificial for computers and requires the addition of an extra transactional effort. Yet the second method is the method by which serious businesses and public administrations natively work, traditionally using paper documents.

After the termination of the session, which is the part of the first method, it may be rather difficult to prove to a 3rd party that the identified user was part of the session and which actions of the computer are attributable to that particular user.

On the contrary, the electronically signed messages, by which electronic signature validation is properly preserved, may survive and serve as evidence to 3rd parties for a relatively long time.

The meaning of Art 3 (1)-(4) is not understandable in conjunction with Art 5 and Art 6. Are such means of identification usable for online interactive sessions? Are they suitable for Art. 19 (1) (b)?

Recommendation: use the terms identification and authentication carefully and clearly; explain that the purpose and desired functionality of Art 5 and Art 6 actually matters.

II.2 Messages signed after reading – messages signed without reading (***)

There is an essential difference in the quality (both legal and non-legal) of signatures attached after less or more careful readings of the document signed and documents that are signed without such care.

In the electronic world, such differences are even more likely to happen. Under Czech law, the circumstance has been solved by two separate legal and technological solutions:

Electronic signature - "electronic signatures" are created under the immediate supervision of the natural person signed. It is assumed that the signatory has read the document and that the document essentially expresses the will of the signatory, which is very important from a legal point of view.

Electronic mark - "electronic signatures" that are those created by automaton on behalf of the person who is considered to be the originator of the mark, as well as of the marked document. Electronic marks express the will of such persons in certain (weaker) ways as well, because that person selected the automaton function, configured the automaton and began its activity. The electronic mark is widely used in practice within the Czech Republic. Electronic marks may be used eg.:

- to sign the invoices of the company that are created in batches
- to sign the listing of the company from the business register, operated by the state
- to sign special receipt messages when the email is received by the public body
- to sign the qualified certificates by CSP
- to sign electronic time stamps by the provider issuing the time stamps...

They could also be used for automatic business transactions, e.g. machines of different companies trading mutually instead of (slow, unreliable, tired ...) human beings.

The term *electronic seal* might be used instead of the Czech term *electronic mark*. However, the concept of the use of the electronic seals in the Proposal is different one than that of electronic marks in the Czech Republic. An electronic seal is considered to be the signature of the legal person. It is doubtful whether this meaning has a strong application need (listed example is signing of the software, however this may be performed by commercial certificates as well).

Recommendation: Certified subject in the qualified certificate for electronic seals is:

- a natural person
- a legal person
- a public authority body.

Further, it should be supposed that the application of electronic seals includes cases where the "electronic signature" is created by automaton, without reading the sealed message.

Note: Natural persons may need the use of automaton signatures as well.

Note: Software still may be signed by the electronic seal of any company (legal person).

II.3 Separate sets of requirements for different types of qualified trust service providers (***)

Trust service providers provide any *trust service* defined in Art 3 (12). Qualified service providers must meet all requirements of the Regulation. Yet most of the requirements listed eg. in Art 19 (2) are aimed mainly at the QTSP, which issues qualified certificates or generates qualified time stamps. Other trust services are likely to have less stringent demands because the associated risks are different. E.g. validation services or electronic signature preservation services may have different demands.

Recommendation: draft the requirements for different types of qualified trust service providers separately and tailor them to the associated risks.

II.4 "Qualified certificate" and "qualified certificates for website authentication" usage (***)

So far, the terms *qualified certificate* and derivatives of it (eg. *qualified system certificate* in Czech law) have been reserved for electronic signatures and related purposes. This was useful, because the related signature creation data (SCD, private key) was considered to be allowed use only for the purpose of electronic signatures and nothing else. This prevented the users from using SCD for other purposes, eg. the SSL sessions. These restrictions protected the signatory against the misuse of SCD.

Art. 38 suggests the introduction of qualified certificates for website authentication. Ie. this certificate shall not be used for any electronic signature purpose but the authentication of the web server which occurs in an online interactive session.

Website authentication is more closely related to the idea of identification, however the technical entity is identified rather than the natural person.

Recommendation: reconsider the usage of the "qualified certificate for website authentication". The certificate could be called in another way, the service remaining the qualified service.

II.5 Lower security of the qualified signature (****)

The Proposal lowers the security of the qualified signature compared with the current state of affairs.

First, the sole control over electronic signature creation data is newly allowed to be only *"with a high level of certainty"* /Art. 3 (7) (c)/. The meaning of this new term is very unclear. May the handwritten signature be written by the hand of the signatory and only under the control of the signatory with high level of certainty? No, of course not. Recital 40 suggests *"It should be possible to entrust a qualified electronic signature creation device to the care of a third party ..."*. While I understand the press of the practice for remotely-stored SCD, this lack of the physical control over SCD may be essential. The sad fact is that the operation of such a 3rd party, which stores SCD and operates the electronic signature creation device, remains UNREGULATED by the Proposal. This, despite the fact that, while *electronic signatures* may operate without *certification authorities* (CSP), the secure implementation of electronic signatures always remains a must.

Second, so far the providers of certification services had to be accredited by the Member states. Newly, only the security audit and its notification should suffice.

Annex II (4) allows the backup of SCD. It is very unclear what advantage there is to the signatory, or anybody else, to backup a SCD? In the case of very rare SCD destruction, the signatory may always create a new SCD and new certificates. The former electronic signature's validity remains untouched by the pure destruction of a SCD.

It is unpersuasive that lowering the security of the qualified signature is a factor in making e-signatures more popular. The objections are:

- relying parties will hesitate to rely on weaker e-signatures
- signatories will hesitate to begin to use e-signatures at all.

Recommendation 1: reconsider whether the relaxation of qualified signature security is proper.

Recommendation 2: if you keep the current relaxation of qualified signature security, then implement all possible measures to protect the signatory by other means, especially cf. II.6, II.7, II.8 and II.9.

II.6 Protection of the signatory – limitation to employer-related relations (****)

Cf. I.2.

Recommendation: In cases where qualified certificates for electronic signatures (for electronic seals as well, if seals are extended by issue to natural persons) are issued because of the primary interest of the employer, whose name is also indicated in the qualified certificate for the electronic signature (or electronic seal), the employee is entitled to limit the use of the certificate to intra-employer relations and/or for outside representation of the employer to 3rd parties and *exclude any other use* of such certificate. The limitation must be included in such certificates and clearly available to 3rd parties.

II.7 Protection of the signatory – limitation to the public law relations (****)

The primary purpose of the entire electronic signature regulation is to enable the signatory to enter into electronic messaging systems used for e-government, i.e. in the relations of natural and legal persons toward the Member State, or its public authorities, and vice versa.

It is not legally proper to force the signatory, who sometimes really must use an electronic signature, because of public law, to bear the risk that his electronic signature may be abused in these private legal relations (which may carry serious financial implications).

Recommendation: Signatories be entitled to restrict the use of their electronic signatures only for communication that concerns public legal relations. The limitation must be included in the related qualified certificate and clearly available to 3rd parties.

II.8 Protection of the signatory – financial limitations on his responsibility (***)

Cf. II.7.

Another possible relief for the signatory is to allow him to set up a financial limit to the private law transactions confirmed by his electronic signature.

The preferable method is a total amount per week or per month. I am aware that this limitation is impractical, but the limit per transaction does not sufficiently protect the signatory. In future, there might be a way to collect information concerning obligations confirmed by the support of specific certificates.

Recommendation: Signatories be entitled to restrict the use of their electronic signatures and related qualified certificates by a financial limit to total amounts per week/month. These limitations must be included in the related qualified certificates and clearly available to 3rd parties.

II.9 Protection of the signatory – precise grace-period definition (****)

The creation of the qualified electronic signature assumes the use of any technical means that are under the control of the signatory. Should the signatory lose such control, he should be allowed to have a specific time period (called a grace period) to revoke his qualified certificate without any legal consequence. I.e. no one should fully reckon on his e-signature prior to the entire grace period expiry. Other security incidents may happen as well (e.g. SCD compromise). However, the common signatory has less chance to note them. Yet it is entirely fair and just to provide such protection.

Many different events must occur during the grace period: the loss occurs, the signatory realizes the loss, the signatory reports the loss (revocation request) to the CSP in a reliable manner, the CSP approves the revocation, information concerning the revocation is transmitted into the revocation system, the information propagates to the revocation mechanism and, finally, after some time this information is provided publicly over the common security means of the CSP to every possible relying party.

Grace periods should be precisely defined, mainly from the point of the view of the signatory. Eg. the signatory may understand " you must report the loss of the qualified signature creation device to the CSP within 24 hours after the real loss occurred".

The relying party may require the precise timing definitions of other parts of the grace period in order to allow an according e-signature validation.

Recommendation: Define the specific grace period precisely, especially from the point of view of the signatory.

II.10 Protecting the relying party in private law communication – preservation of the freedom of contract (****)

The freedom of the signatory to use or not use its electronic signature is guaranteed by his free will. When the signatory is forced to use an electronic signature because of the public law relations or because of his employment, he is protected by the implementation of II.6, II.7 or II.8 limitations.

On the contrary, the relying party is not protected against the electronically signed documents of the communication partners.

Freedom of contract must be preserved. That requires any relying party to remain free to reject any electronically signed documents which may conclude a contract within private law boundaries.

On the contrary, the relying party should be obliged to accept electronically signed documents, provided that a contractual obligation to do so has been established between the parties in advance.

Recommendation: preserve freedom of contract for the relying party.

II.11 Do not give up on WIPIWIS (****)

The Proposal nearly failed on the *What Is Presented Is What Is Signed* (WIPIWIS) principle. While it is clear that the perfect attainment of this goal is problematic with current widely used technologies, it might still be useful to have this principle, at least as the ideal, to be implemented and followed by the implementing and delegating acts.

Recommendation: WIPIWIS should still be forced as the ideal of which attainment is the matter of precise specification by implementing and delegating acts.

II.12 Legal effects claims to be further analyzed (*****)

The Proposal contains several provisions on legal effects, eg. of the electronic signature /Art. 20/, electronic seal /Art. 28/, the electronic time stamp /Art. 32/ and electronic documents /Art. 34/.

These provisions claim ambitious goals. However they should be seriously scrutinized. For lack of the time, this analysis was not included here!

Eg. Art 34 (1) attempts to establish the equivalency of electronic documents and paper documents regarding assurance levels of authenticity and integrity. In fact, any electronic document by itself (without relation to other facts or other documents) has a zero evidence value, even when it is admissible as evidence. On the contrary, some paper documents may include attributes that make them more valuable as evidence from an authenticity and integrity point of view.

Stating equivalency, where equivalency may not actually exist and does not serve any otherwise justifiable aim, contradicts the very principles of the rule of law (or "Rechtsstaat").

Recommendation: further analysis is necessary of the contained legal effect claims.

III. Uncertainties

This chapter lists the objections aimed at specific terms used within the Proposal and which are considered to be possible sources of confusion.

III.1 Electronic document definition (**)

The definition of Art. 3 (27) is unclear. Should it not rather be "any electronic form"? Format is an abstract feature. Does it mean that a document in TXT format, using the ASCII code and printed on paper, is also an electronic document?

Recommendation: make the definition more clear.

III.2 Objective liability of CSP? (****)

The wording of Art 9 (2) resembles the objective liability of qualified trust service providers that might also cover faults performed by other participants. The provider should likely be liable only for the fulfillment of the requirements that the provider himself is obliged to fulfill.

Recommendation: correct the wording appropriately.

III.3 Meaning of the term "online" (*)

In information technologies, the word *online* is usually used in opposition to the word *offline*. Both words occur in the context of services that are geographically separated. Online always means connected IT systems that allow interactive sessions with users. Offline means a service that may only be connected temporarily and the user prepares or transacts the data locally before communication happens eg. only in the batch. In this sense, any website application is online now. Reading and writing email messages is a typical offline service, at least it was in the past.

The Proposal uses the word "online" in a sense that includes both words "online" and "offline", as explained above, at the same time. It may confuse the readers of the Proposal as well as its accurate interpretation.

Recommendation: Consider whether there is not a better term than *online*.

IV. Paradigmatic, philosophical and political issues

This chapter includes the issues having a paradigmatical, philosophical or political nature. This chapter does not contain any recommendations, at most a suggestion.

IV.1 Supervision of the cross-border branches or business partners of TSPs

Art 13 (2) states that only TSPs established on the territory of a Member State are under his supervision. It is questionable whether the branches or contractual partners (eg. registration authorities) of TSPs established in other Member State, although located on the territory of the Member State, should not be the under supervision.

IV.2 Mutual assistance according to Art 14

The conditions of mutual assistance may become matters of dispute. While it may be prudent to allow mutual assistance in certain circumstances, it may also be the source of conflicts.

Suggestion: more precisely define the reasons when requests for assistance is appropriate.

IV.3 Trust service providers from third countries

Art. 10 allows the provision of services of qualified trust service providers, established in third countries, when the agreement to the third country and EU is concluded.

It is not clear why the provision of the services of such providers should have any positive impact on the internal market.

On the contrary when the provision of service is outside the jurisdiction of any EU Member State, the supervision of such s third country TSP by Commission is more complicated.

The real liability of the TSP located in third country jurisdictions may also be questionable.

It may even harm the reputation of the TSPs established in EU Member States.

Suggestion: drop Art. 10.