Digital Policy Alliance
Stakeholders' comments on the proposal for a
European regulation on electronic identification
and trust services for electronic transactions in the internal market

Draft version 1.0 of December 20th, 2012

Industry players providing and using digital signature, authentication and identification services welcome the ambition to build trust in, and enhance the free movement of, such services in the European single market, but are concerned that the proposed Regulation is not the instrument that will achieve this goal. The ten most serious issues identified thus far as affecting in particular the private sector (i.e. without delving into additional concerns that Member States' governments and public sector bodies may have) are the following:

1. **The choice of the instrument in regard of its dual scope**

The proposal combines two very different policy areas:

- on the one hand, the mutual recognition by Member States of the electronic identification means and schemes provided by, on behalf or under the responsibility of other Member States, which is essentially a matter of intergovernmental cooperation;

- and on the other the free movement of digital trust services in general across the EU, which is a purely internal market related question.

Irrespective of whether Member States are prepared to accept a proposal on the internal market legal basis (article 114TFEU) to address the former aspect, industry is concerned that mixing the two areas in one single instrument may play out detrimental to the latter. A not-to-be-excluded lack of political agreement on Chapter II (eID section) would delay or compromise the progress on Chapter III (digital trust services), and undermine legal predictability in a market which, otherwise, does not appear *prima facie* dysfunctional or in need of regulatory intervention. At a time of economic hardship where the growth of the digital single market is seen as a major avenue for crisis exit, holding key enabling services such as digital trust services hostage of such uncertainty may not be the optimal course of action.

Therefore, while the harmonisation and clarity benefits of a regulation are not disputed where single market aspects are concerned, it is dubious whether this instrument is suitable, politically or practically, for the purpose pursued in Chapter II, which would perhaps be better served by a dedicated and separate directive. Indeed, the same level of integration can hardly be expected in areas as different and as far apart as the public administration of public identification credentials on the one hand, and the governance of private digital trust services in the internal market on the other.

2. Uncertainties as to the material scope of the regulation

Article 2 raises a number of questions, especially when cross-read with other parts of the regulation or when confronted to reality.

Paragraph 1 states, among others, that the regulation applies to "*trust service providers established in the Union*". But it fails to indicate whether trust services provided by providers not established in the Union are in scope. A strict interpretation or paragraph 1 might suggest not, and it would be corroborated by paragraph 1 of article 15 which imposes security requirements only on providers established in the Union. But at the same time, that would contradict the spirit of the regulation as enshrined in recital 17 ("*establish a general framework for the use of electronic trust services*") and article 4 paragraph 2 ("*products that comply with this Regulation shall be permitted to circulate freely in the internal market*"), which both seem to cover the service and its use, as opposed to, more specifically, its provision or its provider. And it would also be at odds with paragraph 1 of article 9 according to which all trust service providers, whether established in the EU or not, are liable for their services. From a political perspective, conditioning the liability of the provider on, and therefore subjecting the protection of EU users to, the provider being established in the EU would seem a curious proposition if the purpose is indeed to establish a general trust framework for the use of such services irrespective of their origin.

Paragraph 2 is probably the most cryptic part of article 2. The statement whereby the regulation "*does not apply to the provision of electronic trust services based on voluntary agreements under private law*" is highly puzzling. Technically speaking, this would mean that any trust service provided in a B2B or B2C relationship where no public law requirements apply (i.e. the vast majority of online transactions by private businesses and consumers) is out of scope. However, when confronted with this interpretation, the European Commission claimed that this should be interpreted as a "closed group exception", meaning that it only exempts from the scope of the regulation those transactions that don't potentially or actually implicate any third party. That seems supremely inconsistent with the notion of digital trust services: For the user, the whole point in purchasing a trust service is to be able to use the certification issued by the provider in support of transactions with third parties. In other words, most trust services are not purchased in order to be used in closed groups. For example, a website certificate, provided entirely and exclusively on the basis of a voluntary agreement under private law, is used to ascertain the authenticity of that website to any viewer. Its purpose is intrinsically to be used outside the closed group formed by the user (website operator) and the provider (certificate authority). Therefore, in its current drafting, paragraph 2 raises many questions without answering any.

As to paragraph 3, it states that the regulation "*does not apply to aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form prescribed by national or Union law*". It is unclear what could qualify as "prescribed form", but assuming, for example, that a requirement for "handwritten signature" is a prescribed form for a certain transaction in a certain national law, article 2 paragraph 3 would render the entire regulation inapplicable, undermining in advance its own article 20 paragraph 2 which says that "*a qualified electronic signature shall have the equivalent legal effect of a handwritten signature*". In other words, as per the current drafting of article 2 paragraph 3, all requirements and potential benefits of the regulation could be negated by any national or Union law requirement that would prescribe a form that's not compatible with the characteristics of the digital trust service at hand.

3. Concerns with the free movement of services in the internal market

If we accept that the regulation applies to providers or trust services established in the European Union, then the establishment of a provider (whether it is in the EU or not) conditions the applicability of the regulation, and therefore triggers all the compliance requirements. Notwithstanding the uncertainty as to whether the subject of the requirements is the service, its use, its provision or its provider (or several of these), it is clear that the concept of establishment is an essential one. Yet no definition is proposed. More worryingly still, it has been suggested in informal discussions that for the purpose of this regulation, departing from principles adopted in other pieces of EU law and in EU case law, "establishment" could be understood as meaning the location of the managerial control of a trust service. The implication being that a multinational organisation, otherwise established in the Union by any or all criteria laid down in other legislation and accepted by jurisprudence, could be regarded as non-established in this context if the particular business unit managing the trust services within that organisation happened to be located outside Europe. Were this true, and given the tremendous restrictions proposed in article 10 to the market access of non-established providers[1], this could reveal highly disruptive of current business practices, particularly in an area – the digital market – where services are often provided on a worldwide scale and the physical location of their back office has little or no relevance from an operational standpoint. A clear definition of "establishment" should therefore be included into article 3, matching existing and well functioning principles already accepted and used in EU law.

Moving on, article 4 which lays down the internal market principle creates further cause for industry concern. Paragraph 2 states that "*products which comply with this Regulation shall be permitted to circulate freely in the internal market*". Cross reading this with the definitions of article 3, it appears that

[1] In essence, article 10 restricts the market access of qualified trust services provided by a provider established in a third country by conditioning it upon the prior conclusion between the EU and that third country of an international agreement. How this could work in practice, how this would impact existing practices, how this would tie in with Europe's existing and upcoming free trade agreements, how this would serve the interests of EU businesses and citizens engaging in online transactions on the global digital market, and how this would make the European market attractive for service providers is totally unclear.

the only products which actually have to comply with the regulation are the qualified ones, which then means that, interpreted *a contrario*, article 4 paragraph 2 could actually be used to deny the benefit of free circulation to any service that is not qualified. As this is hopefully not the objective pursued by the European Commission when proposing this article, it is suggested to redraft this paragraph so as to exclude the possibility of any interpretation that would undermine the free circulation of services in the internal market, whether they are qualified or not.

4. Industry concerns with Chapter II on electronic identification

Chapter II is admittedly primarily targeted at the public sector, and governs the mutual recognition of identification means and schemes issued by, on behalf of or under the responsibility of Member States. Irrespective of the concerns that Member States may have with recognising each other's schemes, the industry would like to stress that electronic identification is a service commonly provided on a commercial basis both within the private sector, and from the private sector to the public sector. For example, private sector credentials issued by major providers of information society services (e.g. social networks, webmail services, e-commerce platforms, e-payment service providers) may commonly be used in transactions both with private and public entities. Therefore the new provisions may have indirect or unintended consequences on an otherwise well functioning and growing market, the disruption of which is certainly not the policy objective pursued here. The industry concerns focalise more specifically on the following points:

Article 5, which creates the mutual recognition obligation of all notified electronic identification schemes, does extend this obligation to all services the access to which is subjected to electronic identification by national legislation or administrative practice in a Member State. While the intent is probably to cover only those services which are provided by, on behalf or under the responsibility of that Member State, the actual text does not discriminate between these services, and those provided by private operators but whose access is also subject to electronic identification on the basis of national law or administrative practice (e.g. educational services, financial services, health services, etc.). Which means that in reality, the mutual recognition obligation, meant to be imposed on the Member States, would actually apply also to all private service providers whose services are accessed through a nationally mandated electronic identification mechanism. Given that the technical requirements for the interoperability at the basis of any mutual recognition are left to be defined through delegated acts of the European Commission (article 8 paragraph 3), private service providers who might fall under the mutual recognition obligation don't know any more than the Member States themselves what exactly will be required of them.

Article 6, which defines the characteristics of the electronic identification schemes that Member States can elect to notify (and thus force all other Member States to recognise and accept), imposes on the notifying Member State liability for the unambiguous identification of the natural or legal person prevailing themselves of the eID, and for the availability, online, at any time, and free of charge, of the possibility to authenticate that eID. This liability is unclear in both of its terms: the first one could relate to the identification of the person, to the authentication of part or all of their attributes, or to the

accuracy and uniqueness of their credentials[2], and the second one is very vague as to the actual service levels meant by "*availability of an authentication possibility online, at any time and free of charge*". This becomes critical to private sector operators in two cases:

- when such operators, because of the mutual recognition obligation of article 5, have to use such an authentication possibility, and need – in order to manage their operational risk – to rely on identification means and authentication mechanisms the service levels and associated liabilities of which they neither know, nor control;

- or when a certain Member State, in its domestic market, accepts the use of private sector eIDs (so-called soft IDs) to access certain services. Indeed in this case the question becomes whether that Member State will notify that scheme so as to enable its citizens to use their soft IDs abroad. On the one hand, that would only be possible if the private service were compliant with the requirements of article 6 paragraph 1 (a) to (d), which might require disruptive changes to otherwise well functioning services. And on the other, such notification would force the notifying Member State to take liability for the accuracy and availability of the service towards all other Member States, as per article 6 paragraph 1 (e). In practice, it is highly unlikely that any Member State would accept to take such liability for a service provided by a private stakeholder. Private providers in turn might also find it undesirable to have their services endorsed and taken liability for by any government. Finally, other Member States might be reluctant in practice to recognise private schemes, even if notified by a government. As a result, the proposed architecture for mutual recognition, far from boosting the free movement of eID services in the internal market, could end up hindering it, by discouraging Member States from relying on private services, and by thus distorting and possibly even undermining the otherwise promising market for private eID schemes, which, even if it survived, would become anything but "single".

5. Concerns with the articulation between Chapter II and Chapter III

As mentioned earlier, it is seen as unfortunate that the mutual recognition of public or publicly endorsed eIDs and the free movement of digital trust services are addressed in the same instrument. As described just before, there is also a fear that the proposed arrangement in the eID chapter might harm the market for private identification services. Come to that, it is also concerning that as a result of this dichotomy between eID and trust services, private eID services don't benefit from the provisions applicable to trust services, whereas in practical reality, the provision of eID and other trust services is often integrated and federated, provided off the shelf in one or more components. For example, a

[2] "John Smith is a male, thirty-year old doctor, who was issued the unique electronic identification certificate number ABC123": is the Member State liable for ascertaining unambiguously that the person is John Smith, or for ascertaining unambiguously that this person, whatever their name, is male, or thirty-year old, or a doctor, or for ascertaining that the certificate number ABC123 is attributed unambiguously and uniquely to a certain John Smith, even if the person availing themselves of the eID happens to be Jane Black? Depending on context, any or all of these may be relevant, but the requirement is not clear.

robust and advanced private email service would typically combine an identification component (for access control), a signature component (notably for encryption), a time stamping component (for logging and content management purposes), several functions related to electronic documents and electronic delivery (which are indeed at the heart of the service itself), and would typically be provided through portals which benefit from website certification. Whether all components are supplied by the provider, or whether parts of it are integrated from one or more sub-suppliers, the fact remains that because of the dichotomy, the eID part of that package, even if not unbundled operationally from the rest, would not benefit from the same regime, which is mismatch between the Commission's proposal and business reality.

6. Indiscriminate preference of principle for qualified trust services

As already raised above, the introductory provisions of articles 2, 3 and 4 combine in a way that suggests that only qualified services need to comply fully with the regulation, that only compliant services benefit from the free circulation clause, and that only providers of trust services established in the Union actually fall under (and therefore enjoy the benefits of) the regulation. This is further compounded by the second paragraphs of articles 20, 28, 32, 34, 35, and the whole of Chapter III section 8, which in fact limit the legal presumption of accuracy and trustworthiness to electronic signatures, seals, time stamps, documents, delivery services and website certificates which are qualified. In other words, from a legal standpoint, the message to the users is that any trust service that is not at least qualified (and even better: qualified in itself *and* validated through a qualified validation service, as per article 26) is not trustworthy. This is concerning for many reasons:

Not all transactions require the security and authentication level of a qualified certificate, but these provisions will force the market into either not using electronic trust services, or only using qualified ones even where this level is totally disproportionate to the objective pursued. The counterarguments whereby Member States can require lesser levels of security (article 20 paragraph 4), whereby the Commission may adopt delegated acts to define lesser security levels (article 20 paragraph 6), and whereby users remain free to use non-qualified services if it suits them simply don't stand:

- On the one hand, as already explained, the applicability of the regulation and the benefit of the internal market clause are strongly questionable in regard of those services, and therefore their legal value, even if undoubted in a given jurisdiction, become dubious as soon as a transaction goes cross-border.

- On the other hand, as the presumption of accuracy is limited to qualified services only, the provisions of the first paragraphs of articles 20, 28, 32, 34 and 35 whereby non-qualified signatures, seals, time stamps, documents and delivery services are admissible as evidence is self-defeating: a piece of evidence, which *a contrario* of the respective paragraph 2, is not presumed to be accurate, is not evidence unless proven otherwise. Which is a tautological way

of *de facto* denying any legal value to anything less than qualified[3]. Moreover in the particular case of signatures, article 20 paragraph 2 probably shoots well beyond the target by saying that a "*qualified signature shall have the equivalent effect of a handwritten signature*": the proper parallel with the offline world would be between a simple signature and a handwritten signature, whereas the *qualified* electronic signature would need to be counterpart to a *notarised* handwritten signature (simple signature certified by a trusted third party). This is but one example of the many inconsistencies between the means used to achieve the objectives of the regulation, and the reality it will apply to.

The obvious and unjustified preference for qualified services is therefore likely either to undermine a significant part of the existing market (which is for non-qualified services), or to generate unnecessary costs on businesses and consumers with considerable adverse impacts on e-commerce. The level of authentication implied by qualified services is undoubtedly legitimate and appropriate in many circumstances, but a blanket legal preference for this level will mandate the use of more rigorous authentication that is not necessary in many everyday life situations. In practice, the dilemma for organisations will be to choose between accepting the risk of great legal uncertainty involved in maintaining business processes that rely on non-qualified services, or retooling all existing workflows to accommodate potentially unnecessary, disproportionate and in any case significantly more costly qualified trust services.

7. Sweeping liability provisions on providers of trust services

Breaking away from the status quo of directive 1999/93/EC and also departing from the basic principles of liability in civil law, article 9 introduces a blanket liability of providers for any direct damage caused to a natural or legal person due to non-compliance with the security or other provisions of the regulation, unless the provider can prove it has not acted negligently. What this means in practice is that even if non-compliance as such is not presumed, negligence is, and the causal link between any non-compliance and any direct damage suffered by a natural or legal person is inferred. Meaning, in essence, a reversal of the burden of proof, whereby, faced with a claim of damage due to non-compliance, the provider would have no other option than to prove otherwise. Beside the obvious encouragement of idle claims of damages and vexatious accusations of non-compliance, this arrangement would depart from the proper order of civil law and procure in all legal systems, common law and continental, since times immemorial, whereby it is he who claims a damage and indicates a cause who has to prove the cause itself, the damage, and the causal link between the two.

8. Heavy, potentially disruptive supervision scheme and new red tape

[3] From the user's perspective: The service I invoke is not qualified, therefore if I want produce it as evidence, I can, but I'll need to provide an extra layer of evidence to prove that the first evidence I provided is trustworthy, otherwise it is presumed not to be, i.e. in itself it is admissible non-evidence, a proxy for something, in fact, completely useless.

Section 2 of Chapter III introduces a heavy handed supervision structure composed of to-be-designated national authorities to supervise all trust service providers established in their jurisdiction, and required to report regularly to the European Commission and provide mutual assistance to each other for investigation and enforcement purposes. When it comes to qualified trust service providers, the supervision mechanism foresees not only quite burdensome yearly audits to be reported to the supervisory authority, but also the power for such authorities to conduct additional *ad hoc* audits, and even to issue binding instructions to providers. Industry is concerned that these powers may be disproportionate and potentially even disruptive of business processes beyond what is acceptable and legitimate, not to mention the impact that such forceful interventions as unforeseen audits or the accommodation of binding instructions affecting for example essential aspects of product design may have on business continuity, compliance costs, market prices, service quality or customer satisfaction. It is questioned whether the expected benefits of such strong interference powers are sufficient to balance out the great business risk thus created. In short, such a supervisory structure is in itself a massive disincentive to provide any qualified trust service, which runs contrary to the – otherwise strongly objectionable – intent to force qualified services as the single optimum solution onto all trust service market segments in the EU.

The same is all the more true of article 17 which subjects the market introduction of any new qualified trust service to a burdensome procedure of prior notification involving the filing of a security audit report, followed by a validation procedure before the conclusion of which the provider will already feature on the so-called national "trusted list" described in article 18, but may not yet provide the actual service until the supervisory authority completes the validation. The theoretical period of validation is one month, but the supervisory authority may extend it at its discretion and without limit, simply stating the reason why more time is needed. It is questionable whether such – and so heavy – *ex ante* red tape is indeed required before go-to-market.

Last but not least, on top of the already heavy security requirements imposed by article 15 on all trust service providers (see below), article 19 gold-plates those with an extra set of requirements for qualified trust service providers, the level of detail of which is astounding: they extend from interfering with providers' employment choices to their financial resources and insurance policies, to undefined pre-sale information obligations towards potential customers, to equally undefined record keeping obligations, as well as to mandatory service termination plans the compatibility of which with industrial and intellectual property rules and practices, and with the freedom to do (or to discontinue) business is at the very least dubious[4].

[4] In short, if a qualified trust service is discontinued, the provider is somehow supposed to maintain or hand over the corresponding certificate database to the competent supervisory authority who is in charge (article 13 paragraph 2 (c)) of continuing to serve the issued certificates, which is a questionable expectation both from the provider's standpoint, and from the authority's perspective. A similar issue arises with articles 27 and 31 which mandate the preservation of qualified electronic signatures and seals beyond their technological validity period

9. Oversized security provisions applicable to all trust service providers

Article 15 paragraph 1, in so far as it requires all trust service providers to take security measures proportionate to the risk they face, is sound and welcome. However, the security breach notification requirement laid down in paragraph 2 is highly problematic:

Its trigger, even if set at the threshold of a "*significant impact*", is unclear as the impact is measured on "*the trust service provided and on the personal data maintained therein*". If there is an impact on personal data, the privacy breach notice mandated by the ePrivacy directive, or, in the future, by the general data protection regulation, should apply anyway, while many trust services may not involve personal data at all (e.g. it may be that no personal data is involved in an electronic document, or a time stamp, or a website certificate). Therefore the requirement of cumulative impact on the service *and* personal data is both superfluous and beside the point.

The 24-hour notification deadline is unrealistically short, even to the point of being counterproductive: when a breach is discovered, particularly if it happened on the user's end (e.g. theft of credentials from the user), quite often the investigation of what actually happened and the determination of the real impact takes more time than that, and in many cases, the remediation conducted after the investigation is enough to prevent any significant impact, making the hasty and "tick-the-box" type notification pointless in retrospect.

The recipient(s) of the notification are described very inaccurately, as being "*the competent supervisory body, the competent national body for information security and other relevant third parties such as data protection authorities*". This is by no means satisfactory from a compliance standpoint: who is to say which authorities are relevant in what cases?

Last but not least, as already mentioned earlier, supervisory authorities are conferred the power to issue binding instructions to any trust service provider in order to enforce the security and breach notification requirements. Again, the question is whether such extensive and at the same time vaguely defined powers don't create a risk of disproportionate and disruptive interference with business processes.

10. Reliance on secondary legislation

Last but not least, throughout the 42 articles of the regulation, the Commission is proposing no less than 14 explicit and 3 implied delegations of powers to itself to further specify compliance requirements on providers through secondary legislation, as well as 22 explicit and 5 implied clauses of implementing powers. This raises two issues:

- On the one hand, delegated powers mean that the Commission *may* adopt delegated acts, initiated at its discretion but adopted under parliamentary scrutiny. In a context where

(whatever that may mean), without explaining what outcome is actually sought, or for how long, or what exactly is expected from providers.

technological evolution is fast, uncertainty as to the exact content of the compliance requirements is a source of significant business risk and a strong innovation inhibitor.

- On the other hand, both delegated, and even more so implementing acts, which in turn are adopted without parliamentary scrutiny, could be used to introduce technology specific requirements or actual technology mandates, which should be avoided at all costs, as on top of creating technical market access barriers, these would be unequalled deterrents to innovation, competition, and, in fact, cyber security. Indeed technology mandates freeze specific technologies, services and applications at a particular point in their development, and also create single points of failure. And even if non-technology specific standards are mandated, they might still create geographic market access barriers cutting Europe off from the global market place, or become obsolete for example from a cyber security standpoint long before the procedures to update them can realistically be completed.

Many of the implementing acts are explicitly foreseen in order for the Commission to reference technical standards to govern trust services, the market disruption potential of which is tremendous. At the very least, the delegated powers in articles 20, 21, 25, 27, 28, 29, 35 and 38, the implementing acts foreseen in articles 19, 20 ,21, 22, 25, 26, 27, 28, 29, 33, 34, 36 and 38, and the delegated and implementing acts implied in articles 30 and 31 raise the risk of the Commission setting technology mandates. From an industry standpoint, these are unhelpful both in that they make compliance into an uncertain moving target across the board, and in that they may interfere even to disruptive proportions with otherwise well functioning market dynamics.