

## Position Paper

### on the proposal for an EU regulation on electronic identification and trust services for electronic transactions in the internal market

18.04.2013

Page 1

The Federal Association for Information Technology, Telecommunications and New Media (BITKOM) represents more than 1,700 companies in Germany. Its 1,200 direct members generate an annual sales volume of 135 billion Euros annually and employ 700,000 people. They include providers of software and IT services, telecommunications and Internet services, manufacturers of hardware and consumer electronics, and digital media businesses. BITKOM campaigns in particular for a modernization of the education system, for an innovative economic policy and a future-oriented Internet policy.

#### Background and summary

The Internet and – with it – electronic processes for consumers, businesses, governments and the general public are steadily growing in importance. For reasons of convenience and efficiency, more and more processes are being implemented via web technologies and shifted to the Internet. In this context, and particularly because the risk of identity theft and misuse of personal information has already become part of today's reality, legally binding transactions require secure digital identities. Security experts agree that protecting access to user profiles with user names and passwords will soon no longer be sufficient. Technical solutions, for instance additional security tokens such as smart cards, mobile terminal devices or modern identity documents equipped with chips are already available and will gradually become established in the market. In future, we can hope that Europe-wide standards will also allow us to transact cross-border processes with a reasonable level of security.

In principle, BITKOM therefore welcomes the draft regulation to promote EU-wide use of means of electronic identification.

BITKOM supports the goal of achieving a uniform level of legally secure and privacy-compliant electronic communication. Efforts in this direction will be successful only if legal certainty is guaranteed and therefore if both businesses and private users feel confident that their transactions are privacy-compliant.

Federal Association  
for Information Technology,  
Telecommunications and  
New Media

Albrechtstr. 10 A  
10117 Berlin-Mitte  
Germany  
Tel.: +49.30.27576-0  
Fax: +49.30.27576-400  
[bitkom@bitkom.org](mailto:bitkom@bitkom.org)  
[www.bitkom.org](http://www.bitkom.org)

#### Contact

Nils Hullen  
Head of Brussels Office  
Tel.: +32.2.609 53 21  
Fax: +32.2.609 53 39  
[n.hullen@bitkom.org](mailto:n.hullen@bitkom.org)

Michael Barth  
Head of Department  
Defence & Public Security  
Tel. +49.30.27576-102  
Fax. +49.30.27576-409  
[m.barth@bitkom.org](mailto:m.barth@bitkom.org)

#### President

Prof. Dieter Kempf

#### Management

Dr. Bernhard Rohleder

## **Position Paper**

EU regulation on electronic identification and trust services

Page 2

### **1. In its present form, the draft regulation jeopardises present and future investments in various economic sectors.**

It is evident that incidents of cybercrime, in particular identity theft and misuse, are on the increase. In Germany, reported cases of cybercrime jumped by 16 per cent between 2010 and 2011. In 2011 alone, some 200 million digital identities were stolen worldwide – and this number represents only reported cases. Experts assume that real figures are actually much higher.

More than twenty European countries currently have electronic identification systems in place. These systems protect electronic services offered for the most part in the public sector, but in some cases they also cover commercial applications (banking, retail trade, insurance). Fifteen European countries (Austria, Belgium, the Czech Republic, Estonia, Finland, Germany, Ireland, Italy, Latvia, Norway, Monaco, Portugal, Spain, Sweden, Switzerland) use two-factor authentication systems for improved security.

In its present proposal, the regulation would force countries where businesses, government ministries and public administration departments met the challenges of providing safe digital identities at an early stage by creating a suitable legal framework and developing and introducing appropriate solutions to come up with new plans to handle the range of identification and security levels used by the various Member States in the government and industrial business processes based on these systems.

The main goal of any efforts made in this area should be to provide adequate security levels. As mentioned in the introductory section of the draft regulation, security mechanisms such as “username / password” should no longer be used, especially for critical processes like identification. The authentication level developed in the EU “STORK” project could provide a bridge towards a swift EU-wide universal use of higher security levels. The draft regulation fails to take this into sufficient account.

### **2. Because it offers too little planning security, the draft regulation hampers significant innovation and investment.**

The market for terminal devices and the range of mobile services and applications on offer in the Internet will continue to grow dramatically. At the same time, innovations in the field of mobile solutions also drive the need for innovative security features and processes. An EU regulation should not be allowed to impede innovation in the field of these important security functions.

The proposal currently gives the EU Commission the right to enact “delegated acts” on most of the issues. Moreover, because they are not formulated precisely enough, some articles of the proposal open up too much leeway for interpretation.

## **Position Paper**

EU regulation on electronic identification and trust services

Page 3

The resulting uncertainty means that investments will be postponed until the legal environment has been sufficiently clarified.

Besides the Member States listed above, other EU Member States and/or candidate countries have announced national eID programmes. These are, for example, Poland, Hungary, Slovenia, Romania, Croatia, Norway and France. Although risks are increasing – as we have already pointed out – and with them the need for safer solutions to protect digital identities, it seems likely that these programmes will now be abandoned or postponed as a result of the planning uncertainties created by the EU draft regulation. There is an urgent need for clarity in the individual aspects of the issue and for adequate security standards for providers of trust services, for government authorities and for industry.

The EU draft regulation does not adequately address the issue of uniform safety standards, e.g. for trust service providers and identification services. Instead, the Commission intends to regulate these services by introducing implementing acts at a later stage (cf. Art. 15 (6), Art. 17 (5), Art 19. (5), Art. 38). It is not clear when such subsequent legislation might be enacted, nor are the contents of the implementing acts clear, as the proposed regulation establishes no substantive framework for them.

For the providers of trust services as well as for the identity provider industry, this approach creates a significant degree of economic uncertainty, as it obstructs essential business planning processes. The same uncertainty also affects users: government authorities, industry and normal citizens.

Specifically, the consequences of this uncertainty are that every subsequent specification of technical requirements and standards applying to trust service providers, every subsequent decision on forms and procedures of monitoring by yet-to-be determined supervisory bodies will be likely to cause additional expense for facilities, personnel, processes and documentation – costs that cannot be passed on directly to the user of the electronic services. The EU draft regulation gives no indication of what measures might be necessary or of when they might be implemented. We therefore recommend a significantly more precise wording of Articles 16, 17 and 19.

In our opinion, the mutual recognition and interoperability of the security procedures intended by the draft regulation between entities of different countries in which heterogeneous solutions have already been introduced will, in the absence of a common framework and standardised security norms, be nearly impossible to achieve. For example, in order to handle all possible forms of an access process, a company or government department would have to offer a number of different access methods, introduce mechanisms to cope with the effects of various levels of security in the subsequent business processes and bear the costs of their implementation and operation. In order not to impede market access and competitiveness of the companies involved, the implementing acts planned in the regulation should therefore be based at least on existing

## Position Paper

EU regulation on electronic identification and trust services

Page 4

(open-source or proprietary) standards and tested solutions that offer adequate security levels.

The EU proposal fails to set either minimum insurance coverage requirements or liability limits for trust service providers. This would be necessary for the protection of both consumers and providers.

The role of so-called ‘third-party contractors’ who assume tasks on behalf of trust service providers is not sufficiently regulated. This should be more clearly specified in the EU regulation. Liability limits should also apply to entrusted third parties.

Some Member States already operate identification systems that are based on entirely different philosophies. All of these electronic identification systems have varying security mechanisms for identification and authentication (mutual authentication, access mechanisms, encryption, etc.) and contain differing sets of user data and data formats. This means that **substantial upfront investments** will be required that initially cannot be assessed in any economic analysis. In countries with high numbers of EU foreigners, for instance Germany, this could mean that 27 or more different electronic identification systems of trust service providers would have to be supported. The draft regulation fails to show how this could be handled, although EU projects such as the ICT large-scale pilot project “STORK”, which involved the participation of most EU countries, have already developed solutions to these problems.

### 3. The draft regulation ignores proven, existing standards and fails to define an adequate level of security.

What EU members actually need is an EU-wide technical mechanism for verifying eIDs and e-signature tools, something that cannot be achieved merely through mutual legal recognition of heterogeneous IT systems. Mutual recognition in the absence of defined and comparable security levels encourages the parties involved – following their own economic interests – to be satisfied with the lowest common denominator, a tendency that severely inhibits the innovative forces that are so important in this area.

So far, reasonable security requirements have not been taken into account by the current draft. This should be corrected for two reasons: first, a comparable economic evaluation of identity systems is not possible without agreed security parameters. Second, the lack of appropriate security standards also represents a threat to the interoperability of the different systems.

Identity definitions such as the ‘IDABC authentication level’ defined by ENISA, which are already in use in EU projects such as STORK, should be mentioned in the EU regulation. An AAL3 specification, or, even better, AAL4, would be desirable from the point of view of acceptance by EU citizens. Security requirements

## Position Paper

EU regulation on electronic identification and trust services

Page 5

relating to products should be defined on the basis of the internationally harmonised Common Criteria.

#### 4. The draft regulation must take into account the objective of promoting acceptance of electronic identities among public administrations, in industry and by ordinary citizens.

##### a) Attribution of identification data to persons in connection with basic data protection principles

From Chapter III (Trust services) onwards, the draft EU regulation takes data protection concerns into account. These issues are not yet reflected in Chapter II (Electronic identification), although this is an area that both normal citizens and the business world view as being much more sensitive. This is probably because the topic is so new.

Requirements of “privacy by design”, i.e. linking data to a specific purpose in order to achieve data economy and data avoidance, are not yet mentioned at all in this catalogue of requirements.

What is needed is, for instance, a situation where personal information can be managed on the basis of need, so that only required data is actually transferred.

Social networks and access solutions in industry and banks often use **pseudonyms** instead of users’ real names. In terms of data protection, and more specifically, in terms of data economy, this is a very desirable function that should be encouraged. The EU draft regulation does not allow this function for identification purposes (cf. Article 6, paragraph c). In our opinion, the present EU draft regulation is inadequate in this regard.

Many Internet services require only an **age verification**, for instance for the protection of minors. It is not the date of birth itself which is transmitted, but only a confirmation that the user has reached the requested age. Similarly, downloading games, programs, new software versions, etc., does not require the transmission of names or addresses. For purposes of data minimisation, the EU regulation should take such **anonymised** services into account (supplement to Article 6 paragraph c). This should also include electronic voting, to the extent that this is permitted by law.

From the point of view of the industry, chapter II of the EU draft regulation is too limited: it fails to take into account pseudonymous and anonymous applications or age and address verifications. For privacy reasons, these options should be considered as a way of minimising data. Multiple identities or roles should be permitted.

## **Position Paper**

EU regulation on electronic identification and trust services

Page 6

### **b) Understandable framework**

For many users it is very important to know their communication partners. Especially when personal data is required, some users are highly sensitive, while others are not.

A system that deals with personal data should be acceptable to ALL user groups alike. The work of Internet fraudsters should be made as difficult as possible. It should be noted here that any national or EU-wide system of identity management should have the fullest possible trust among all the groups involved and be well received by the media.

Special attention should be given to mutual identification, particularly when third parties might be involved in the communication – which is a fully normal assumption in the Internet.

Systems that transport confidential data will not be accepted on a permanent basis until all the parties involved know who their communication partners really are.

The introduction of qualified website certificates mentioned in Article 37 of the draft could meet the security needs of private and commercial users; such certificates should then, however, be required at all times for the retrieval of personal data.

These certificates are useless in their present form, as only recognition by the Member States is stipulated; in reality, such certificates work only when used by providers of services, for instance for online shopping.

### **c) Uniform data set**

For communication across national borders, a set of personal data must be defined that can be used for essential business processes in all Member States. So far, the draft does not address this issue.

Every process requires specific data. Most government processes, for instance, require a user's first and last names. Some processes also require a person's name at birth.

From the point of view of data privacy, however, the data set might contain too much data – for instance for use in commercial contexts.

For example, a personal data set might contain a social security number or other similar information, so that, under German law, there are many processes for which this means of identification could not be used.

To ensure user acceptance and EU-wide application, a set of data that offers the users legal certainty and trust should be defined.

## Position Paper

EU regulation on electronic identification and trust services

Page 7

### **5. The provisions of the proposal dealing with transitional periods must be reconsidered**

As technical and organisational requirements will be decided only in delegated and implementing acts, setting a date for the provisions of the regulation to come into force in relation to the date of publication of the regulation itself is problematic. Instead, the implementation period should be based on the date of publication of the delegated acts, as it is not until then that the actual requirements will be known and regulated.

In some cases, the requirements applying to operators of trust services can have a profound effect on their security concept and on the design of their business processes. It is therefore important not to underestimate the time and cost of implementation. Whilst the Commission's proposal provides for a transitional period for already issued qualified certificates and signature creation devices (Article 41), it does not provide for a transitional period for the operators of trust services, so that here requirements must be implemented within twenty days of the publication of the regulation (Article 42).

In the area of trust services, implementation of technical and organisational requirements should be allowed transitional periods of at least one year from the date of publication of the complete specifications, and not, as currently provided for in the proposal, twenty days from publication of the regulation.

No transitional periods are planned in the area of electronic identities. According to Article 7 (2), the Commission would publish the list of notified eIDs six months after entry into force of the regulation. As the regulation merely provides a framework for notification, the specific form of notification (within the framework of notification requirements and of the delegated and implementing acts) remains national competence. This means that before a national eID can be notified, national law may need to be adjusted once the regulation has entered into force or after publication of delegated acts.

In the sensitive area of the processing of personal data, the legislative process should be carried out with due care. In order to avoid any distortion of competition in this adjustment phase, the initial list of notified eIDs should not be published by the Commission until after a suitable transitional period. The length of this period should be calculated so that all national eIDs can be adapted both legally and in terms of technical or organisational aspects to the requirements of the regulation in advance of its initial publication. Such a transitional period could – depending on the necessary adjustments – be two years.

## **Position Paper**

EU regulation on electronic identification and trust services

Page 8

### **Individual articles:**

#### **1) Art. 2 (2) Scope**

This provision is unclear. The “voluntary agreements under private law” mentioned here apply to the vast majority of German CSPs. The process of identifying an entity as belonging to the group addressed by this draft regulation requires complicated derivations and interpretations and must therefore be clarified.

It is not clear, for instance, whether a commercial service that gathers identification data with the help of a state identification system such as a national ID card and uses it for an identification system of its own which is also subject to some degree of legal regulation should be covered by paragraph (1) or (2). The definitions that follow in Article 3 only serve to further complicate the issue. In principle, this problem affects the majority of European postal services.

#### **2) Art. 3 (30) in conjunction with Art. 37 Definition of a qualified certificate for website authentication**

The draft regulation unfortunately does not specify clearly what purpose these certificates could have in addition to the usual SSL certificates normally stored in browsers. To be included in browser lists, providers of SSL certificates must pass WebTrust or ETSI certifications and are then shown by the browser as secure.

Qualified certificates for website authentication do not currently meet this requirement. After the certification process, they are therefore included in the browser list in the same manner as other certificates, including non-European ones.

Mutual authentication (for instance at a hotel reception) means that the user knows without a doubt who is asking for his personal data. This provides the basis for a self-determined, confident manner of dealing with personal data.

Therefore, use of these new certificates – in the same manner as the German authorisation certificates – could be made compulsory for the retrieval of personal data by means of the notified identification systems.

Such a measure would give users the opportunity to verify who wants to access their personal data, opening up the possibility of enforcing data and consumer protection requirements. The restriction to website authentication should therefore be abandoned, and the provision should be extended to cover all web service providers who use a notified identification system.

A possible next step would be to obligate all web services to provide technical data protection for their users' personal data.

The concrete technical design (X.509, CV) should be regulated nationally and be suited to the identification service.

## **Position Paper**

EU regulation on electronic identification and trust services

Page 9

### **3) Art. 5 Mutual recognition and acceptance, in conjunction with Art. 6 Conditions of notification**

The mutual recognition and acceptance system will perpetuate the current problem of lack of EU specifications affecting some areas with regard to appropriate security requirements for the ID systems of the Member States. Even though we can expect EU Member States – acting in their own interest (e.g., liability or fighting black money or terrorism) – to apply normal standards of security in the development of their eID systems, specific stipulations would be very welcome.

For online business transactions, this special need for appropriate security standards is a result of the lack of personal presence, as invisibility removes the psychological hurdle to abuse. The use of national identification systems in the fight against black money requires particularly high security requirements. In Bitkom's view, clarifying the liability issue would be a welcome step.

### **4) Art. 6 I d) Compulsory availability of free authentication possibilities**

This article makes the notification of national systems contingent on the possibility of free authentication. If commercial services such as those described in '1) Art. 2 (2) Scope' are covered by the regulation, this creates a problem for provider companies.

Authentication processes cost money. If companies are forced to offer these processes free of charge, however, their willingness to offer them at all will sink.

If there are reasons that have led to this extremely counterproductive provision, they should be rigorously reviewed to see whether strict price regulation is really necessary and what applications it should be limited to.

Depending on the interpretation of the scope of application, however, the present draft creates an incalculable cost risk for provider companies, which would mean that national systems may not be notified at all.

This would totally destroy the entire system of identification services.

### **5) Art. 8 Coordination**

From today's perspective, simply mandating coordination is not sufficient. It would be desirable to designate an entity, for instance ENISA, which could act as the driving force behind such coordination.

### **6) Art. 9 Liability**

The limitation of liability for trust services to damage caused by negligent acts brings the liability requirements for trust service providers up to the level of

## **Position Paper**

EU regulation on electronic identification and trust services

Page 10

general practice in Germany and can therefore be viewed as progress. A specific minimum amount of insurance should be defined across the EU in order to create a level competitive playing field.

### **7) Art. 17 Initiation of a qualified trust service**

The provision according to which certificates issued under the terms of Art. 20 (2) have the equivalent legal effect of a handwritten signature and under Art. 20 (4) must be accepted throughout the European Union as soon as the qualified trust service has notified its operation places heavy demands on the system for validation of qualified certificates, as the supervisory body will not necessarily have access to all notifications received in the EU if there are delays in the transmission of trust lists to the Commission. There is a short time window in which no reliable validation is possible. Thus, the receiver (the validating body) cannot be sure whether the service is indeed a qualified trust service in the European Union. Legal force should thus be contingent on publication in the trust lists and not on notification.

### **8) Article 19 Requirements for qualified trust service providers**

Art. 19 of the EU proposal fails to set either minimum insurance coverage requirements or liability limits for trust service providers. This would be necessary for the protection of both consumers and providers.

### **9) Art. 19 (2) g) Requirements for qualified trust service providers**

Recording relevant information is useful, but the provision is not clearly formulated. Here the minimum information to be recorded should be specified, as legal proceedings would not necessarily take place in the land of the trust service. A question that could come up, for instance, is how to find out after ten years who is the person behind a certificate? There should also be an identical EU-wide process for storing the pertinent information after a qualifying trust service has ceased to operate (for example, transfer to the supervisory body, etc.).

### **10) Art. 22 Requirements for qualified electronic signature creation devices**

It would have been very helpful, at least in the explanatory comment to the draft regulation, to mention the existence of standards such as prEN 14169 and EN 14890.

## **Position Paper**

EU regulation on electronic identification and trust services

Page 11

### **11) Art. 38 Exercise of the delegation**

For most articles, the Commission may publish ‘delegated acts’. In other words, the provisions made here are not rigid; they can always be changed by new regulations. The impact on products already issued, on products in manufacturers’ warehouses and on products under development is unclear. See also DIN comment 8 and DIN comment 2.

### **12) Annex II Requirements for qualified signature creation devices**

The requirements of Annex II are similar to the requirements of Annex III of EU Directive 1999/93/EC. There, however, there are no minimum requirements with regard to security evaluations or algorithms. Until now, this has been achieved by national legislation, something which is no longer possible as a result of point (15) of the EU draft regulation. This could reduce the level of security of secure signature creation devices. See also DIN comment 9.

### **13) Annex IV Requirements for qualified certificates for website authentication**

In contrast to (b), users of qualified certificates for website authentication in (c...e) can be only legal persons. This must be an editorial error.

## **Position Paper**

EU regulation on electronic identification and trust services

Page 12

### **Annex –**

#### **Comments from the working bodies of DIN e.V.**

(German Institute for Standardization)

DIN, the German Institute for Standardisation, is a private organisation with the legal status of a non-profit association. DIN members include companies, federations, government agencies and other institutions from industry, commerce, trade and science.

Altogether, some 28,000 experts contribute their expertise to the work of creating standards. Pursuant to an agreement with the Federal Republic of Germany, DIN is the competent German standards organisation for both European and international standardisation activities.

Remark: This draft being for an EU regulation, the regulation itself will apply directly in all German states as soon as it enters into force. Because EU law prevails over national law, one can certainly say that the national laws and regulations affected by the new regulation, for instance the German Signature Act [Deutsches Signaturgesetz] and the German Signature Ordinance [Signaturverordnung], are being 'replaced' (cf. also Chapter 3 of the draft).

1.) Point (21): Technological neutrality. This could weaken the position of the signature card as a smart card.

2.) Point (49): The regulation would give the Commission the power to adopt acts on various aspects. It is unclear what modalities would need to apply for these legal acts to be adopted (simple majority, unanimity, ...). See also the comment on Article 38 at number 8.

3.) Point (15) of the draft is unclear. "This rules out any specific national technical rules requiring non-national parties for instance to obtain specific hardware or software to verify and validate the notified electronic identification." What would be the effect of this provision on the validity /applicability of technical guidelines (e.g. BSI), algorithms catalogues (BNetzA, BSI), the requirement of having to use specific card readers for signature generation ('comfort readers'), etc.?

4.) Article 15: A security concept for trust service providers does not seem to be mandatory. This could lead to a reduction in security standards for trust service providers compared to the current situation in Germany.

5.) Article 19: There does not seem to be any defined minimum insurance limits or liability limits for trust service providers. Moreover, liability is typically passed on to entrusted third parties. This could mean unlimited liability for a card manufacturer.

6.) Article 20: Point (17) would restrict the scope of application in such a manner that laws with explicit formal requirements are excluded (e.g. testaments). However, this is not reflected in Article 20.

## Position Paper

EU regulation on electronic identification and trust services

Page 13

7.) Article 23: A confirmation ('certification') in accordance with the signature requirements still seems to be available as an option, but it is not mandatory. According to point (15) of the EU draft regulation, however, no government is allowed to make this type of certification mandatory.

8.) Article 38: For most articles, the Commission may publish 'delegated acts'. In other words, the provisions made here are not rigid; they can always be changed by new regulations. The impact on products already issued, on products in manufacturers' warehouses and on products under development is unclear. The composition and above all the conditions for the adoption of a legal act are not clear (simple majority, unanimity, etc., cf. also comment to point (49) above).

9.) Annex II: Requirements for qualified signature creation devices: basically very little has changed in the requirements. However, no mandatory security evaluation is required (cf. also Art. 23). In the case of Annex III of EU Directive 1999/93/EC there was also no specific requirement for a security evaluation, but the published standards (in particular prEN14169) suggested it. There is no reference to a catalogue of algorithms. Until now, these aspects were regulated by national legislation. According to point (15) of the EU draft regulation, this will no longer be possible, thereby potentially reducing the level of security compared to the situation in Germany today.

10.) The role of third-party contractors for trust service providers is discussed explicitly only for the act of registration. It is therefore unclear whether card manufacturer as authorised third parties may perform services such as key generation on the card or not. This could represent a limitation of the value chain of card makers.

11.) Result: It seems that the new regulation would significantly reduce the formal minimum requirements for secure signature-creation devices (safety evaluation is not mandatory, no reference is made to algorithm catalogues or technical guidelines that must be complied with, and point (15) of the EU draft regulation seems to indicate that regulation via national legislation is no longer possible. There is, however, a reference to standards that can be published in the EU Official Journal, cf. Article 22).