bitkom

Position Paper

EBA consultation to the regulatory technical standards on strong customer authentication and common and secure communication under PSD2

12.10.2016

Federal Association
for Information Technology,
Telecommunications and
New Media

Dr. Frank Termer
Head of Software
P +49 30 27576-232
f.termer@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Thorsten Dirks

CEO
Dr. Bernhard Rohleder

Bitkom represents more than 2,400 companies in the digital sector, including 1,600 direct members. With more than 700,000 employees, our members generate a domestic turnover of 140 billion Euros a year, exporting high-tech goods and services worth another 50 billion Euros. They produce hardware and consumer electronics or operate in the sectors of digital media and the network industry. 78 percent of the companies' head-quarters are located in Germany with an additional amount of 9 percent in other countries of the EU and 9 percent in the USA as well as 4 percent in other regions. Bitkom supports an innovative economic policy by focusing the modernization of the education sector and a future-oriented network policy.

Introduction

Bitkom welcomes the opportunity to answer the EBA Discussion Paper on future Regulatory Technical Standards on strong customer authentication and common and secure communication under PSD2.

Bitkom considers that the regulatory framework in the European Union is an adequate environment for business and innovation in the area of e- and m-commerce, including payments. EU legislation on payments, e-money and consumer rights is among the most advanced globally, and serves as examples for many countries around the world that want to achieve similar market integration, innovation and prosperity. This holds also for the European payments market. Bitkom strongly supports the initiative to foster a single European market for retail payments and protection of consumer interests. Bitkom is certain that the prospect of economic reward is the key driver for innovation.

The pace of development in payments innovation has increased significantly with the development and increasing prevalence of the internet and more recently multi-functional smartphones. The evolution is still ongoing and any final scenario cannot be predicted. Regulatory neutrality must be respected as regards the various types of payment systems and methods. Bitkom therefore insists that any regulatory interference deemed necessary must not disrespect regulatory neutrality.

General remarks

The digital transformation is one of the greatest challenges of our time. Innovation cycles decrease and speed of change increases. Within digital platform economy speed and agility are general conditions and main factors of daily business. Therefore companies are forced to behave equally quickly and strategically in the digital transformation of their business. By doing so existing jobs can be secured and new ones can be created. Digital transformation does not stop at industry boundaries and it is already an ongoing process, e.g. in the automotive, banking, media, pharmaceutical industry or in tourism, agriculture or aviation.

One key aspect for a successful transformation of a company is a central strategy for every field of digitization. A well-defined digital strategy should be holistic and take into account changes in technology, competition and personnel requirements. Strategies for the use of digital technologies in only some certain areas are not enough. With a constriction on individual aspects of digitization there is the danger of neglecting the development of fundamentally new business models. These disruptive developments are innovations which change markets fundamentally, by replacing existing products or services.

Digital technologies increase productivity and the competitiveness of our economy. Digitization is a basic requirement for retaining and creating jobs. When it comes to obstacles for digitizing, for most companies regulation is one main factor and innovation can be hampered by excessive regulation. In finance, the smartphone becomes a hub for banking transactions. At the same time the number of branch offices decreases dramatically. In ten years customers will pay with smartphones and wearables in stores. In many shops not even a cash desk will be needed. In addition, a majority of finance managers say cash will no longer be the dominant method of payment.

Against this background it is necessary that the RTS specifies system-agnostic requirements for the interfaces with its elements, components and message types. ASPSPs should provide technical documentation based on the minimum requirements specified in the final RTS and help TPPs to rapidly adopt the various interfaces for its services. There must be minimum barriers to be complied by all PSPs and hence to foster a European Open Banking ecosystem.

Therefore, to be effective, the RTS need to be made in this context

- balance between security/authentication and convenience
- impact on competition, not just between banks, but between new entrants, FinTechs and non-bank PSPs
- digital environment in which consumers operate, the digital devices they use and the network connectivity that is available
- different needs and business models (including new business models) of merchants, which are diverse and changing

Beyond the consultation questions, which will be answered below, Bitkom wants to point out the following with regard to the regulatory technical standards on strong customer authentication and common and secure communication under PSD2:

- It is of great importance that the possibility of outsourcing the authentication process to e.g. MNOs as set out in Article 12 is ensured. This is especially true for provisions that affect the pragmatic implementation of this outsourcing process. For example the current text in Article 12 (b) mandates the PSP to digitally sign the software used to authenticate a transaction. This requirement is too specific and should be changed mandating the integrity of the software must be protected without requiring specific technologies.
- Mandating the use of digital signatures for the end to end process would default all transactions to LoA4 and its requisite infrastructure. This highest standard possible may rule out customers in markets that deploy a SIM based solution (applet) without NFC SIMs. Also LoA4 is not necessarily translating into best security because it focuses on technical components instead on overall security for the system. Instead similar to eIDAS-regulation LoA3 (level "substantial"), according to ISO 29115 for authentication LoA3 could be set as a minimum requirement. Bitkom believes that for payments conducted under the PSD2, the LoA3 is sufficiently secure. The best way forward here is to start similar to eIDAS-regulation with a minimum requirement of LoA3 according to ISO 29115 enhance it with additional network information (greatly enhancing security, e.g. SIM Swap) and over time move to LoA3 using additional security features as the industry and consumers develops.
- In general the reference to the eIDAS-regulations (EU regulation 2014/910) is too weak. For example more references to the Levels of Assurance (Article 8 of eIDAS (and refinement in 2015/1502 / EU) could be made (see point above).
- The current requirement for independence of authentication elements is likely to unnecessarily preclude the mobile device as a possession element. The current provisions of these draft RTS cannot be met by a well-functioning authentication process, because different ways of achieving independence are currently ignored by these RTS.
- It is important to rely on internationally accepted principles on privacy and data protection. In order to protect stakeholder's privacy solutions should use proper mechanisms such as encryption and PCR (Pseudonymous Customer Reference).
- Bitkom would like to have more definitions included in the RTS (e.g. LoA, first time, tamper resistance).
  - LoA: as defined in ISO 29115
  - first time: What is meant here? The first time using this device, this application, the current channel?
  - tamper resistant: Should be removed altogether as a requirement because that requirement is not technology agnostic as it requires hardware. The RTS should require a risk based approach to protect the credentials in Article 9.
- In general the RTS should not set the requirements at an extremely high standard as this would lead to a situation where people would not use mechanisms. A balance between the necessary security and customer usability has to be found.

Consultation questions

3.2.1 The requirements of the strong customer authentication

Q1: Do you agree with the EBA's reasoning on the requirements of the strong customer authentication, and the resultant provisions proposed in Chapter 1 of the draft RTS?

Bitkom supports the endeavour of EBA to refrain from providing too many further detailed rules to strong customer authentication procedures, where PSD2 requires the use of two independent factors out of knowledge, possession and/or inherence elements. EBA should not interfere with the endeavours of the industry to develop at the same time secure and convenient authentication procedures. It is good to note that EBA advocates the possibility to adopt strong customer authentication procedures based on the services of a public e-identity scheme under the eIDAS-regulation framework; these possibilities are currently explored by many PSPs and technical service providers.

However, in general Bitkom fears that the draft guidance on SCA is able to hamper the development of e-commerce in Europe. The RTS is too narrow and prescriptive, which will introduce friction in the customer experience and place additional burdens on merchants and PSPs. This will divert investments away from the development of innovative authentication procedures. PSPs should be allowed to develop innovative authentication solutions that are both secure and convenient, by 1) allowing behavioural data to be used as an inherence element within the SCA framework, and 2) by making the use of an authentication code optional, in line with the requirements in the PSD2. This flexibility in the application of SCA would benefit both consumers and merchants and help achieve a Digital Single Market in the EU.

1) Behavioural characteristics can include transaction history, habitual location, device used, preferred retailers, and other consumer habits that the PSP is able to collect, in accordance with EU data protection and privacy rules. Because these attributes are collected and assessed over a period of time, they are less susceptible to theft, spoofing, malware, or malicious replication than other elements in the SCA procedure. Behaviour-based characteristics have been successfully used by PSPs to identify cases where control of an account was lost or compromised, and it is increasingly accepted throughout the industry that behavioural evidence can be used as an independent inherence element.

2) The RTS goes beyond the requirements in the PSD2 by requiring that SCA results in the generation of a once-only authentication code: authentication codes are not mandated in Art. 97 of the PSD2, and recital 96 notes that SCA "may result in authentication codes such as one-time passwords": they are therefore mentioned as just an example amongst other. Strong Customer Authentication as defined in the PSD2 can be delivered through the combined use of independent, secure, static authentication elements (e.g. passwords, device-specific certifications or credentials, biometrics etc.) without the need for one-time authentication codes. Requiring their use simply adds friction to the customer experience, with no real security benefits.

Bitkom suggests that the RTS should be open for technological development and it is premature to rule out (in general) any technological standard. It is certainly understandable that EBA requires in its proposed RTS periodic testing of the strong customer authentication procedure for each PSP. This is imperative from the perspective of risk management and control. However, EBA should emphasize that the criteria for the audit must be the risk assessment of the PSP and the audit should not require that any authentication method is 100% bullet proof. Therefore there

should be minimum requirements defined for the technical separation of the different authentication elements (device's operating system and the mobile application receiving resp. generating the authentication code on the same device). It needs to be ensured that innovative authentication elements and methods are not discriminated.

Generally spoken Chapter 1 of the draft RTS is very detailed, so that Bitkom wishes to see a preference for caution. Basically the chapter is acceptable. Article 6 of the draft RTS provides the independence requirements. These requirements allow sufficient space for future technical developments, which is to be welcomed. Nevertheless, a more concrete control / embodiment to existing and established technical devices in the payment process would be helpful. At least the setting of minimum requirements for the separation of the different authentication elements would be helpful. It should be ensured that no business model is excluded.

Basically, Bitkom agrees to the EBA that PISP (and AISP) can rely on an existing authentication method of ASPSP in strong customer authentication (paragraph 19 a). This is also governed by Article 97(5) within PSD2. Nevertheless, this passage cannot be found in the articles of the draft RTS again. Generally understood, ASPSP would be responsible for implementing the authentication procedure because the authentication will be performed by the systems and processes in the context of the ASPSP despite involvement of third services. Here, further clarification would be helpful including a specification on the extent of reliance on ASPSP's SCA procedures with regard to security mechanisms.

Furthermore the phrase "tamper resistant" should be defined more specifically (see points 26 and 30 in the consultation paper) or removed from the RTS. Previously the term is defined neither in the PSD2 nor in the draft RTS. One possibility could be to make a more precise definition by referencing to existing definitions to have the most homogeneous understanding. This should be made under the aspect of consistency within Europe.

Additionally the exclusion of "behavioral data" is critical (see paragraph 29 in the consultation paper; it is not included in the RTS). Behavioral data should not be evaluated as inherent data and behavioral data should not be categorically ruled out for the future. Much more it should be re-examined on an individual case according to actual state of the art of technical possibilities. Maybe one approach could be to describe threat scenarios. For example "behavioral data" could - as of today –be considered as an element for potential smart SCA-exemption solutions and not only as an on top tool for fraud prevention.

Regarding Article 7 it should be specified what would happen if the review of auditors would come to the conclusion that the system is not sufficiently resistant. Bitkom would suggest to include a risk analysis rather than to describe legal consequences. The result of the auditors has to be considered within the risk analysis. EBA should define minimum requirements for the report that will be made available for auditors. What are the thresholds and rules that would trigger a security issue? In case, the system is not sufficiently resistant, there should be a clear process in place with a mitigation plan

One last point concerns the handling of bulk transactions. Here not only the view of private financial customers should be taken, but also the companies' view is important. It should be clarified if the Electronic Banking Internet Communication Standard (EBICS) is included or not.

Q2: In particular, in relation to the "dynamic linking" procedure, do you agree with the EBA's reasoning that the requirements should remain neutral as to when the "dynamic linking" should take place, under the conditions that the channel, mobile application, or device where the information about the amount and the payee of the transaction is displayed is independent or segregated from the channel, mobile application or device used for initiating the payment, as foreseen in Article 2.2 of the draft RTS.

Bitkom agrees with the reasoning that the requirements should remain neutral as to when the "dynamic linking" should take place. Bitkom agrees as well with the approach of the EBA that smartphones and tablets (generally "mobile devices") can be used simultaneously as an authentication element and for storing and reading other authentication elements. It must be ensured at the smartphone, that the individual functions of the device function independently and thus the risk of compromising is attenuated (paragraph 30).

Q3: In particular, in relation to the protection of authentication elements, are you aware of other threats than the ones identified in Articles 3, 4 and 5 of the draft RTS against which authentication elements should be resistant?

As already written above, Bitkom wishes to have regulations which are not misleading, but even as concrete as it is necessary to have legal certainty. A necessary specification than is made by the economic implementation. Any over-regulation should be avoided. Regarding the several points listed here, it should be reflected on an acceleration date for each feature. Regarding this, Bitkom would like to make a concrete proposal for one point: In Article 5 change "... algorithm specifications, biometric sensor and template protection features..." into "... algorithm specifications, robustness of biometric capture devices against presentation attacks and template protection features...".

The RTS needs to specify what biometrics technologies should be supported (e.g. fingerprints, face and voice recognition, iris scan) and what security requirements should be fulfilled by the ASPSP to store these sensitive data. Bitkom realized that "behavioral data" is not included in the RTS and should not be completely excluded. There are multiple highly innovative companies developing authentication methods using behavioral data and hence help improving user convenience and experience.

3.2.2 Exemptions

Q4: Do you agree with the EBA's reasoning on the exemptions from the application of Article 97 on strong customer authentication and on security measures, and the resultant provisions proposed in Chapter 2 of the draft RTS?

Bitkom wants to question, if the designation of explicit numbers is desirable. No one can say how the Euro is developing. What is about Non-Euro-countries? What is the baseline there? Bitkom wishes that there should be a basic structure so that companies do not have to explore own borders. But there should also be the possibility of extending the limits based on own considerations. So consequently numbers should be used as a baseline, but they should not be specified as absolute. This method would consider existing market dynamics. Another possibility would arise when taking a customer perspective. In conjunction with the whitelist, a customer could determine own limits which would give greater transparency and self-determination.

Furthermore the limitation in Article 8 (1 b ii) of the draft RTS should be determined with respect to "cumulative amount". It is not clear from the current wording, how the "cumulative amount" of 150 EUR should be determined.

Does this limitation refer to the use of a single payment instrument or to a plurality of payment instruments? Or is there a time limit, e.g. monthly? The same question also arises with Article 8 (2 d ii) of the draft RTS.

Bitkom suggests to include an exemption for bulk payment (in particular via EBICS): While EBA has included in the draft RTS the exemption for a series of credit transfers, this only applies if the amount and the payee is the same, i.e. for recurring credit transfers. EBA does not – at least not explicitly – exempt credit transfers which the payer wishes to authorize as a bulk. Therefore, it would be sensible to require only one strong customer authentication per each bulk credit transfer. This possibility would be particularly important for treasurers or accounting departments of enterprises which usually collect credit transfers during a day and will authorize and send those in a bulk (in Germany often using EBICS). While EBA in its general observations (on dynamic links) seems to contemplate that strong customer authentication must be applied only once for the entire bulk, this is not expressed in the draft RTS. It would be helpful, if EBA could add an explicit exemption in the RTS for such bulk credit transfers. Otherwise PSD2 would require a strong customer authentication for every payment transaction of the bulk.

Bitkom also suggests including an exemption based on a transaction risk analysis of the payment service provider: Next to these enumerated exemptions, it seems odd that EBA has not included the transaction risk analysis. In particular in comparison to the white list-exemption, where the payer must do its own "beneficiary risk analysis" EBA should give PSPs that flexibility. The 10 EUR exemption for remote electronic payment transactions seems to be an extremely cautious replacement. It seems that EBA is afraid of a varying interpretation of such an exemption in the different jurisdictions which would cause a fragmentation of the European payments market. This, however, seems exaggerated. EBA would be able to provide to the competent authorities of the Member States a sufficient set of rules for interpreting such an exemption; also EBA in collaboration with the EU Commission would be flexible enough under PSD2 to renew and to amend the RTS if the market developments may give rise to concerns.

Bitkom thus recommend aligning article 8 with the reality of digital payments by ensuring a robust risk-based approach, together with exemption thresholds that are aligned with the PSD2 and reflect the e-commerce market reality. Bitkom does not understand the basis and the rationale for the remote electronic transactions exemption thresholds in Chapter 2. A limit of 10 EUR per transaction (and 100 EUR cumulatively) would oblige users to go through the unfriendly experience of SCA for almost any digital payment, regardless of the actual risk posed. This approach will have a detrimental impact on e-commerce, which would be at odds with the EU Commission's efforts to foster the digital economy's growth in the EU. We therefore suggest aligning the thresholds to match that of those for low-value transactions in Art. 42 of the PSD2.

The RTS should in fact rather encourage PSPs to develop and put in place risk-based authentication capabilities that would allow PSPs to select the most effective authentication challenge based on the level of risk of transactions: i.e. the RTS should introduce an exemption based on a transaction-risk analysis. The RTS should define auditable risk management procedures, measuring outcomes and enabling the ASPSP's home state regulator to evaluate their effectiveness using metrics reported by PSPs (e.g. risk of the underlying payment instrument, the risk profile of payer and payee and the risk of the transaction context, like the habitually used device).

The RTS states that the AISP shall not be exempted where the payer accesses the information of its payment account online, or the consolidated information on other payment accounts held, for the first time or later than one month after the last day in which strong customer authentication was applied. In case of multiple information requests in a

short time period, the user won't be asked for strong customer authentication and enter user credentials and authentication code each time data is requested. In order to enable TPPs such as FinTechs and PSPs to develop successful user-friendly applications and avoid frictions, there is a clear need of a technical mechanism and infrastructure at the ASPSP's side to cater this function (such as Tokenization Services).

> **Q5:** Do you have any concern with the list of exemptions contained in Chapter 2 of the draft RTS for the scenario that PSPs are prevented from implementing SCA on transactions that meet the criteria for exemption?

With regard to the list of exemptions it is actually not clear whether these exemptions are mandatory or not. Bitkom suggests clarifying that the exemptions should not be mandatory: In its Consultation Paper EBA further raised the question whether the exemptions should be mandatory for the PSP or not. If mandatory, the PSP would not be allowed to apply strong customer authentication in these cases. This would seem correct if the exemptions will be available only for strictly defined payment methods and amounts. The white list exemption would be acceptable as mandatory if the PSP has the right to reject the payer's (its customer's) selection of beneficiaries.

Nevertheless, in this context the liability aspect should be taken into account. If the PSP of the payer does not require strong customer authentication this will shift the liability for (allegedly) unauthorized payments towards this PSP; the onus of proof of the PSP becomes more difficult to fulfil. As long as PSD2 does not lessen the burden of proof for the PSP in exempted cases it should be the responsibility of the (card issuing, the account servicing etc.) PSP to decide whether or not to apply strong customer authentication. Bitkom believes that every PSP should be able to decide on its own, based on a risk analysis, because of the legal responsibility.

Bitkom recommends that the list of exemptions proposed in Chapter 2 (i) is kept optional and (ii) is reviewed on a regular basis to avoid that it becomes obsolete in the fast-paced Internet environment. PSPs should be allowed to modulate deployment of SCA according to the actual risk of the transaction, given that the PSD2 identifies the "level of risk involved by the service provided" as the first criteria based on which the exemptions to SCA should be determined by the RTS (Art. 98.3). PSPs should be able to apply more or less stringent security based on specific and pre-approved risk-metrics. Since fraudsters are extremely sophisticated and increasingly fast in breaching security methods, it is key that PSPs are allowed the flexibility to adapt their security response to the cyber threat.

3.2.3 Protection of the confidentiality and the integrity of the payment service users' personalised security credentials (PSCs)

> **Q6:** Do you agree with the EBA's reasoning on the protection of the confidentiality and the integrity of the payment service users' personalised security credentials, and the resultant provisions proposed in Chapter 3 of the draft RTS?

Bitkom sees an advantage in clarifying definitions to relevant terms. Some terms, e.g. personalised security credentials or sensitive payment data, are defined within Article 4 in PSD2, but these definitions are very broad and are therefore hard to use. EBA should clarify what confidentiality means in Article 9 and that e.g. abuse of PSCs by PSPs administrators SCA should be hard or impossible. The RTS should cover the whole lifecycle of the PSC. Bitkom would suggest definitions which are consistently across the EU. A clear remark by EBA that they approve of the

general understanding of "sensitive payment data" as limited to data that can be abused for fraudulent online payments, would already imply a welcome clarification benefit for market participants.

3.2.4 Common and secure open standards of communication for the purpose of identification, authentication, notification, and information

> **Q7:** Do you agree with the EBA's reasoning on the requirements for common and secure open standards of communication for the purpose of identification, authentication, notification, and information, and the resultant provisions proposed in Chapter 4 of the draft RTS?

Bitkom supports the approach of EBA that every account servicing PSP will have to provide at least one communication interface enabling secure communication with payment initiation service providers, account information service providers and PSPs issuing card-based payment instruments. That interface must be documented and freely available on the account servicing PSP's website. Also, they require that this communication interface must use common and open standards which are developed by international or European standardization organizations, such as ISO 20022. However, the described interfaces, mechanisms and formats (ISO20022 or other industry standards) need to be specified in terms of minimum technical requirements – e.g. basic mechanisms and minimum field level information. This will make it less complex to implement these interfaces at the TPP's side. A balance between minimum requirements and flexibility is desirable.

EBA provided in the draft RTS for the principle of equal treatment of such overlay service providers and any payment service user: this means that the communication interface which the account servicing PSP is offering to those overlay service providers must have the same functionalities and the same level of availability, including support, as the online platform made available to the payment service user. Further, the draft RTS require that the data elements made available by the account servicing PSP must consist of the same information as the information made available to the payment service user.

In paragraph 19 a) of the draft RTS it is noted that PIS and ASPSP can sign a contract that gives the PIS authorization to use their own credentials, agreed with the client, to authenticate the client. This possibility should also be given to the AISP. Any technical specification of the communication interface should be made available for free and publicly on the website. It is important that the documentation is available in English as the main language in payments generally is English.

> **Q8:** In particular, do you agree that the use of ISO 20022 elements, components or approved message definitions, if available, should be required to ensure the interoperability of different technological communication solutions implemented between PSPs for the provision of AIS, PIS or for the confirmation on the availability of funds? Do you see any particular technical constraint that would prevent the use of such industry standards?

Bitkom agrees to the usage of industry standards.

Q9: With regards to identification between PSPs, do you agree that website certificates issued by a qualified trust service provider under an e-IDAS policy would be suitable and allow for the use of all common types of devices (such as computers, tablets and mobile phones) for carrying out different payment services?

Bitkom concurs with EBA that a definition of sensitive payment data is not feasible as it varies from payment method to payment method. But regarding Article 20 (3) of the draft RTS it should be presented more clearly what is meant by "the role of the payment service provider". After formulation, it can be assumed that a third PSP may have different roles and can specify in which role he undertakes services (as AISP or PISP) when executing specific services. It is unclear why the role of the third party PSP should be stored in the certificates used for identification. On the basis of the certificates, the role cannot be recognized. Additionally the lifecycle of a role can be different. Similarly, the third party PSP should identify itself as the sender of the job to the ASPSP. The regulation in its current draft version is designed not quite clear at this point.

Q10: With regards to the frequency with which AIS providers can request information from designated payment accounts when the payment service user is not actively requesting such information, do you agree that the proposed limit of no more than two times a day achieve an appropriate balance between allowing AISP to provide updated information to their users while not negatively impacting the availability of the ASPSP's communication interface? If not, please indicate what would be in your view the appropriate frequency and rationale for such frequency.

Bitkom wants to make clear that a regulation with a hard limit of a two times frequency may not be sustainable. Even if one thinks on push-services. A customer can use more than one service provider so that a push-service with only two times frequency is not very useful. Multiple data retrieval should be possible at the request of customers. This should be designed in a way that the customer can grant permission to the AISP for the repeated data retrieval without instructing him explicitly every single time. Bitkom suggests maintaining the two times frequency as a minimum requirement, but it should be allowed to use multiple data retrieval with no upper limit, especially with regard to the possibility of other techniques in the future. Article 22 seems to be more concerned to prevent harm from the ASPSPs and does not contain any provision to prevent harm from the user. The RTS should require that data exchange without the user being present must be limited to prevent PSP from creating user profiles. The user's consent to request information without the user being present should not only be rate limited but also time limited as well and the consent should automatically expire after a time not longer than one year. The time limit on the user consent to retrieve data without the user being present must not be automatically extended when the user is present but the consent must be explicitly expressed by the user.

A perfect approach would be to leave the definition of quantitative retrieval access limits fully to the hands of the user by empowering the user to configure this in the AISP's and/or the bank's system user interface. Such a procedure would be more conforming to the EU-GDPR which must not be neglected in the context of PSD2. In extension of question no. 10 it would as well be strongly recommended to empower the user to define which types of transactions (e.g. cash withdrawal, electronic payment, digital payment) and which data segments of those transactions (e.g. recipient and/or amount of transaction) may be visible/analysable for the AISP. Again, this is strongly induced by the EU-GDPR. Bitkom suggests that the ASPSP should provide the user with an access control function in order to manage all access rights that were given to TPPs to access the payment account. This access control function should be specified in the final RTS.