e-ID: emerging business cases – boosting uptake

Possible synergies between PSD2 and the eIDAS Regulation

Geoffroy Goffinet
Consumer Protection, Financial Innovation and Payments

Agenda

1. The mandate in the PSD2 : Focus on identification in relation to the common and secure open standards of communication (article 98.1.d)

2. Questions raised in the Discussion Paper and answers received

3. Potential synergies with e-Idas.

The mandate in the PSD2

Focus on identification in relation to the common and secure open standards of communication (article 98.1.d)

Mandate

- The PSD2 confers a mandate (art 98.1.d) on the EBA to develop in close cooperation with the ECB the requirements for common and secure open standards of communication for the purpose of identification, authentication, notification, and information, as well as for the implementation of security measures, between account servicing payment service providers, payment initiation service providers, account information service providers, payers, payees and other payment service providers.
- In particular, the PSD2 framework foresees that AIS, PIS providers will have to identify themselves with the ASPSPs every time a payment is initiated or for each communication session (Article 65 (2(c)), Article 66 3 (d), Article 67 2(c)).
- These requirements will also apply for the confirmation of availability of funds between an issuing card-based payment instruments' PSP and the ASPSP (Article 65).

Questions raised in the Discussion Paper and answers received

Questions raised in the Discussion Paper and answers received

EBA could consider clarification in its future regulatory technical standards on the following aspects:

- The way AIS, PIS providers will have to identify themselves towards the ASPSPs for access to payment account information (e.g. exchange of electronic certificates, see as well chapter 4.5), and every time a payment is initiated including the purpose for which the AIS and/or PIS is authorised by the PSU and requesting access to the ASPSP upon each connection. Such requirements could clarify whether or not trusted third-parties need to provide assurance (e.g. in the form of security assertions) about the identification of entities involved in such communication.

Answers received on Q15, Q16, Q17 and Q20 can be summarised as follows:

- Broad consensus for the use of certificates (such as SSL certificates) for ensuring identification between ASPSPs, PSPs issuing card-based payment instruments, AISPs and PISPs.

- Many answers highlighted some difficulties to use e-idas certificates, in particular due to the liability regime behind the framework that may not be compatible with the liability regime under PSD2. Against this background, many market participants supported the fact that e-idas certificates could be a solution but shall not be required under the future EBA RTS.

Questions raised in the Discussion Paper and answers received (fin)

Answers received on Q15, Q16, Q17 and Q20 can be summarised as follows:

- In relation to the use of trusted third-parties to provide assurance (e.g. in the form of security assertions) about the identification of entities involved in such communication, diverging views were expressed:
  - Some market participants suggested that the future EBA register should provide these certificates : THIS WILL NOT BE THE CASE!!!! To be noted: the EBA register will have no legal basis (only Home Competent Authority register will be legally binding),
  - Some market participants suggested that certificates should be issued by a certification authority or third party ensuring that the PIS/AIS provider is licensed.
  - Some other market participants suggested that the future RTS should describe a procedure for the exchange of certificates that should ensure that identification of licensed entities is ensured.

Potential synergies with e-Idas

Potential synergies with e-Idas

- Website certificates issued by a qualified trust service provider under an e-idas policy that would in particular include :
  - ✓ the name of the institution,
  - ✓ its licensing number,
  - ✓ the competent authority that has delivered the license,
  - ✓ the role of the PSP (AIS,PIS, both PIS and AIS, PSPs issuing card-based payment instruments or ASPSP).

- **Pros :** qualified trust service provider issuing the website certificate would verify for a legal person the name of the legal person to whom the certificate is issued and, where applicable, the registration number as stated in the official records and would take liability in case of oversight. In addition, the certification authority is itself subject to supervision to ensure that it performs its verification properly.

- **Question:** it is not yet clear whether any certification authority will have applied for the status of Qualified trust service provider under e-idas by the time of implementation of the draft RTS (i.e. October 2018 at the earliest).