The security levels specified by the eIDAS Regulation for electronic means of identification (eID) are only suitable to a limited extent for use in the sovereign area of the member states. In particular, according to the current legal situation, the unauthorised transfer of an eID (in Germany, e.g. Union citizen card and PIN) cannot be detected. This often stands in the way of integrating eID in the sovereign sphere, since acting under a false identity cannot be ruled out with certainty. This problem could be solved by including a further security level in Article 8 (e.g. high+), where a significantly higher level of security could be achieved through the mandatory comparison of a biometric photo in the context of a video conference. As a result, eID technology would have a much broader scope of application in the public sector in the future, since national authorities could dispense with the need for citizens to appear in person even in sensitive areas.

With regard to the security levels of electronic identification systems, it should be made clear that the "four-eyes principle" can also be applied for (initial) identity verification of a person. For example, trust service providers should be allowed by law to require that the applicant present his or her identity document to another independent body prior to verification by the trust service provider. It would therefore be desirable if the Implementing Regulation (EU) 2015/1502 of 8 September 2015 laying down minimum requirements for technical specifications and procedures for security levels of electronic identification means pursuant to Article 8(3) of the eIDAS Regulation could set out requirements in this respect.

Unfortunately, compliance with the security-relevant requirements of the eIDAS Regulation (and its implementing provisions) in the area of qualified electronic signatures (qeS) varies greatly from one European country to another. Thus, national solutions are on the market in which the identification of the signatory by the respective qualified trust service provider is not very reliable and thus little is done to prevent misuse. Since such solutions are placed comparatively cheaply on the market, predatory competition and thus a "race to the bottom" is to be feared, which could discredit qeS as a whole in the medium term. It would therefore be desirable if the Commission would, on the one hand, tighten the requirements for the individual security levels and, on the other hand, control the national supervisory bodies more closely.