Technical Standards Provision	Description	Commentary
Chapter 1 **Strong Customer Authentication**	• Sets out security requirements for each of the two or more elements required for SCA, namely knowledge, possession and inherence. There are also requirements that these are independent of one another so that a breach of one does not compromise the others. • Explains that the application of SCA results in the generation of an authentication code for customers characterised by security features including, but not limited to, algorithm specifications, length, information entropy and expiration time. • With respect to making "electronic remote payment transactions" using SCA and elements that dynamically link the transaction to a specific amount and payee (or possibly a unique identifier), technological solutions must ensure the confidentiality, authenticity and integrity of this information, and that *the means of displaying it should be independent or segregated from the application used to make the payment*. • For card-based payment transactions, where the customer has agreed to "ear mark" a specific sum (e.g., car hire), the authentication code must be specific to the maximum amount.	Aside from favouring a principle-based approach as opposed to a more prescriptive one, the EBA has weighed what it regards as the competing demands of customer protection and the need to ensure fair competition between PSPs. The need to have a separate authentication window for "electronic remote payment transactions" (i.e., independent or segregated from the application used to make the payment) will potentially discourage the use of smart phones to make payments. Authentication within the app used to make the payment will not be allowed. The EBA consider there is flexibility as the authentication code could be a single piece of data inputted on the interface of the PSP by the customer or, for example, generated from several items of data including a one-time password. The RTS requirements on dynamic linking are different to those in the EBA's Guidelines. Applications may need updating. The EBA has rejected calls to allow "transaction risk analysis" as a basis for allowing exemptions from SCA, as lacking a reliable means of validating the data. The EU Parliament has taken issue with this approach.
Chapter 2 **Exemptions from Strong Customer Authentication under the current draft of the RTS**	• Exemptions from the need to carry out SCA are provided in a limited number of cases as follows. • Where the payer makes a contactless electronic payment transaction at a point of sale which does not exceed €50, nor cumulatively more than €150 without application of SCA. • Where the payer makes a credit transfer online and the payee is included in a list of trusted beneficiaries previously created by the payer with its account provider. • Where the payer makes online a series of credit transfers in the same amount and to the same payee. • Where the payer makes an online credit transfer and the payer and the payee are the same natural or legal person and the payee's payment account is held by the	The EU Parliament considers it is unclear from the draft standards whether the exemptions are optional or mandatory. A number of these have been carried over from the EBA's 2014 Guidelines. The EBA itself has questioned the scope of payment instruments that are subject to the requirement to use SCA. PSD2 refers to electronic payments initiated by the payer (e.g., credit transfers or card payments), but not to electronic payments initiated by a payee only, such as direct debits, which might in future grow in popularity as a result. The EU Parliament wants to see higher maximum limits for contactless payments and considers that insufficient weight has been given to the negative impact on PSPs of the proposed thresholds.

	payer's account provider (an inter-account transfer). • Where the payer initiates a remote electronic payment transaction (e.g., via the internet or for example, a mobile phone) which does not exceed €10, nor cumulatively more than €100 without the application of SCA.	Similarly, the Parliament has questioned the proposed maximum amount of €10 for remote electronic payment transactions and has called for an increase in the limit. It also questions if the cumulative limit is workable as some transactions take place "online" and others "offline." The proposed threshold would impact retailers which offer customers one click payment such as retail high-tech giants. A failure to use SCA, (assuming their PSP was willingly to carry out the transaction), would place payment risk with them. The EBA considers that the lower threshold compared to contactless payments, reflects the higher susceptibility to fraud of remote electronic payment transactions.
Chapter 3 **Personalised Security Credentials**	• Provides that the confidentiality and integrity of customers' PSCs shall be ensured at all times during authentication including display, transmission and storage. • To this effect PSC (1) should be masked when displayed and not readable to their full extent, (2) should not be stored in plain text, (3) and any secret cryptographic material related to its encryption should be stored in secure and tamper resistant devices and environments. • The security measures should ensure that only *that* customer can use the PSC and authentication devices. • The delivery of PSCs, authentication devices and software to customers should be carried out in a secure manner to guard against the risk of unauthorised use due to their loss, theft or copying. • Security measures employed should be documented, periodically tested, evaluated and audited by internal or external independent and certified auditors.	The Bank Stakeholders Group had opposed direct access of PSC by payment initiation and account information service providers. In any event, the EBA state that they have adopted high-level principle based requirements for PSCs to facilitate competition and adaptability. PSPs providing acquiring services will need to ensure that their contractual documentation with retailers incorporates these security measures to protect PSC. These provisions have much in common with the Payment Card Industry Data Security Standard (PCI DSS) used by major card schemes.
Chapter 4 **Communication Standards**	• Sets out requirements regarding identification between PSPs and requires that there are processes in place to ensure that all payment transactions and other interactions with customers are traceable. • Account providers with payment accounts accessible online must offer at least one *communication interface* to enable payment initiation and account information service providers and PSPs issuing card-based payment instruments to	As for granting payment initiation and account information service providers access to customer accounts, the EBA has decided to give "sufficiently concrete guidance" and in doing so (in the Parliament's view) appears to favour a single technological solution to the development of principles for access. The Parliament is concerned that a mandatory "dedicated interface" may allow account providers to exclude or

	identify themselves, communicate securely and to rely on their authentication procedures. • Account providers are to ensure that their communication interface uses ISO 20022 elements, components or approved message definitions, if available, as well as standards of communication which are developed by international or European standardisation organisations. • For the purposes of authentication, PSPs are to use website certificates issued by a qualified trust service provider under e-IDAS (Regulation 910/2014 on Electronic Identification and Trust Services for Electronic Transactions). • Account providers should ensure that communication interfaces operate at the same level of service, including support, as online platforms used by their customers when directly accessing accounts online. • PSPs should ensure when exchanging data via the internet, that secure encryption is applied to safeguard the confidentiality and the integrity of the data using recognised encryption techniques. • Account providers must (1) provide account information services with the same information from designated payment accounts and associated payment transactions as made available to customers when directly accessing their information online, provided this does not include the display of sensitive payment data; (2) payment initiation services with the same information on the initiation and execution of payment transactions as available to customers when directly initiating a payment transaction; and, (3) provide confirmation by means of a simple "yes" or "no" answer to PSPs on the sufficiency of funds for the execution of a card-based payment transaction.	limit "direct access" to a customer's account by payment initiation and account information service providers. It considers this runs contrary to the objectives in PSD2. The EBA has stated that neither PSD2, nor its mandate, specify the nature of the access or that it should be "direct access" (however defined). Further, that the draft RTS do not prescribe whether access should be through the account provider-customer interface or a "dedicated" interface specifically created for this purpose, but merely the principles governing access. ISO 20022 is one of a number of standards already in use for payments. There may be cost implications for those PSPs which need to transition over to it. As for the authentication of PSPs requiring access, recognising that the technical standards will not apply at the earliest until October 2018, the EBA have assumed, that one or more qualified trust service providers under e-IDAS will have been designated where there are none now. The EBA have said that e-IDAS will need to be considered on case by case basis to see if it will deliver compliance. Secure encryption must be applied to communications, although there is no reference to any standard, nor any requirement for an agreement between PSPs which might make provision.