PSD2 Compliance - Q&A

Q: How do hardware-based solutions such as OTP tokens provide dynamic linking with single transactions?
In general, users can enter payment information such as the amount of money and the beneficiary account number into hardware tokens. This can happen via the keypad of the token, via a USB cable or by scanning a visual code. The hardware token can then use the payment information to calculate an authentication code according to the dynamic linking requirements.

Q: Can the combination of mobile and token be counted as a two channels and be PSD2-compliant?
According to PSD2, the authentication mechanism must be constructed from two out of three possible authentication elements, i.e. something only the user has, something only the user knows, and the something only the user is.

Q: Does this mean VASCO supplies the dynamic linking? Not another entity such as PSP?
It is the responsibility of the PSP to perform strong authentication of its users. VASCO can provide PSPs with products and services to perform strong authentication.

Q: When would you use the authentication code? Do you consider it as a second factor?
The authentication code must always be used to authenticate a user. The authentication code must be generated by an authentication mechanism that is constructed from two out of three possible authentication elements, i.e. something only the user has, something only the user knows, and the something only the user is.

Q: Would the usage of PIN and fingerprint be sufficient for generating the authentication code?
According to PSD2, the authentication mechanism must be constructed from two out of three possible authentication elements, i.e. something only the user has, something only the user knows, and the something only the user is. A PIN is something the user knows, and a fingerprint is something the user is, so this could indeed be sufficient.

Q: How do you comply with the requirement in Article 2(2) a) when a customer makes several payments together to different payees?
In case of bulk payments, the authentication code must be calculated based on the total amount of money of all payment combined and based on the account numbers of all beneficiaries.

Q: If exemptions are used, is it correct that SCA in total can be skipped and not just dynamic linking?
That is our understanding as well.

Q: Can you discuss TRA for bulk payments?
In case of bulk payments, the authentication code for SCA must be calculated based on the total amount of money of all payment combined and based on the account numbers of all beneficiaries. There are no specific provisions about TRA for bulk payments.

Q: Does RASP protection cover the cloning protection?
VASCO's DIGIPASS for Apps provides a device binding feature that offers cloning protection for mobile apps.

Q: Has VASCO received formal assurances from ECB regarding the compliance of their tokens with PSD2 RTS?
At this moment, there is no formal certification program for specific products under PSD2. As such, it is not possible for VASCO to obtain formal assurance. However, VASCO discusses compliance of its products in informal ways with competent authorities in order to make sure we correctly interpret the RTS and to make sure our products comply.

Q: Do we understand correctly that all PSPs need to have TRA, even if they plan to use SCA for all transactions? If so, what is the rationale behind this requirement in your opinion?
Indeed, PSPs always need to use TRA even if they use SCA. TRA provides a second layer of security, next to SCA. TRA is useful to protect against social engineering attacks, whereby an adversary tries to convince the genuine user to confirm a payment using SCA when the payment is actually fraudulent.

Q: Is 3D secure protocol for cards enough for SCA or is it mandatory?
3D Secure is indeed a protocol which can be used by PSPs to build a solution to comply with the SCA requirements for card-based payments.

Q: Is dynamic linking the same as transaction signing?
Yes, it is. The wording "dynamic linking" is used by PSD2 and the RTS on SCA.

Q: Can a prevention solution by VASCO gather all types of transactions, including: e-banking, card, POS, mobile banking, wallets etc.?
Yes, VASCO's IDENTIKEY Risk Manager can be used to analyze transactions for different types of payment channels.

Q: What is VASCO's opinion of the RTS for corporate banking?
The RTS on SCA provide minimum security requirements for authenticating users. In case of corporate banking, users typically perform payments of relatively high amounts. Therefore, we expect banks to protect their corporate banking applications with authentication mechanisms that are stronger than required by the RTS on SCA.

Q: What category of the 3 elements of SCA can you give to OTP over SMS? Is this knowledge or possession?
The user receives the SMS message normally on a personal phone, so this would be a possession element.

Q: Could you clarify the scope of PSD2? Is it only internet payments (browser-based online)? If not, what else?
PSD2 covers browser-based and mobile payments.

Q: The RTS is requiring channel separation between the application that will use the OTPS and the OTPS transmission. How do you see 1aa compliant?
The final draft RTS does not require channel segregation anymore. As indicated in the comments in the final draft RTS, this language was removed from the draft RTS because it was confusing.

Q: To access payment accounts, the RTS allows the 1 Factor Authentication only after the first time. Access performed with a valid 2 FA should be performed again every 90 days. This is not what you have been presenting, could you explain?
Article 10 of the final draft RTS states that payment service providers are not exempt from the application of strong customer authentication to payers who want to inquire about their balance or consult their payment history from the last 90 days if either one of the following conditions is met: (a) the payment service user is accessing online their account balance or payment history from the first 90 days of paragraph 1 for the first time; (b) the last time the payment service user accessed online their payment history from the past 90 days of paragraph 1 and strong customer authentication was applied more than 90 days ago.

Q: I understand that SCA is not necessary with the first time and after 90 days when TRA is implemented. Is that correct?
TRA always needs to be applied to every payment.

Q: How do you see the usage of behavioral parameters as authentication factors?
Yes, we see this as a possible inherence element. The comments from the EBA to the final draft RTS also indicate that this is possible.

Q: Do the directives or guidelines define certain mandates for 2aa and 1aa solutions in case the physical medium is lost or stolen?
The final draft RTS states that the authentication procedure should include, in general, transaction monitoring mechanisms to detect attempts to use a payment service user's personalized security credentials that were lost, stolen, or misappropriated. This applies to all authentication solutions, not just those in the 2aa or 1aa category.

Q: What are the requirements if the customer already has a list of beneficiaries certified with SA but has to make a money transfer with a different value?
As indicated in Article 13 of the final draft RTS, SCA is not required for payments to trusted beneficiaries. For the precise conditions, please consult the article itself.

Q: Do you need RASP when using an SMS solution? SIM app?
The mobile device where the SMS arrives might also contain an authentication app (in the 1aa or 2aa scenario), where the SMS needs to be entered. This app would need to be protected using RASP.

Q: Does the PSU have to see the payment details (amount & account) on the token? What you see is what you sign?

"See What You Sign" on hardware tokens can be used to comply with the Dynamic Linking requirement, but it is not the only option. Displaying the data in a mobile app is very likely to be acceptable as well.

Q: Do you see the Universal Windows Platform (UWP) and Windows tablets as a viable solution platform for SCA in a 2aa or 1aa setup? Is the sandboxing different from iOS/Android?
The sandboxing techniques of Universal Windows Platform (UWP) are similar to Android and iOS. UWP adopted many of the concepts from Android and iOS. Windows 10 Mobile allows running UWP apps only, so the sandboxing mechanisms are of comparable strength as Android and iOS here. Standard Windows 10 allows running both UWP and regular Windows applications, so the sandboxing is less strong than Android or iOS.

Q: Could you be more specific about multiple transaction signing/authorization possibilities? Does Dynamic linking allow multiple transactions / beneficiaries?
The final draft RTS states that, in case of bulk payments, the authentication code must be calculated over the total amount of money of the payments, as well as information about the beneficiaries of the various payments.

Q: We have a hardware DIGIPASS 275 with 5 numbers that can be used as a challenge response for dynamic linking. Is this compliant for Dynamic Linking?
Challenge/response by itself is not sufficient to meet the Dynamic Linking requirement of PSD2. The authentication code must be calculated over the amount of money and beneficiary ID of the transaction, so these two items must be provided as input to the device.

Q: Is Dynamic linking still necessary for payments below 30 EUR in case of transaction monitoring solution implementation?
No, dynamic linking is not required for payments below 30 EUR, as long as the cumulative amount, or the number, of previous remote electronic payment transactions initiated by the payer since the last application of strong customer authentication does not, respectively, exceed EUR 100 or 5 consecutive individual remote electronic payment transactions.

Q: Can payments be whitelisted? If we validate destination for the whitelist and then we allow payments without DL to that destination, should it be sufficient?
Article 13 of the final draft RTS allows the payment service provider not to perform strong customer authentication if the payer initiates a payment transaction where the payee is included in a list of trusted beneficiaries previously created. See Article 13 for the details.

Q: If two-app authentication is used, do both mobile apps need to use sandboxing OS and RASP?
Sandboxing is applied by the OS (e.g. Android or iOS) of the mobile device to every app running on the device. RASP should be applied to the authentication app.

Q: If for an application, the hardware identifier, fingerprint, PIN, need to be combined, is there a recommendation for an HMAC algorithm?
We recommend using standard HMAC algorithms, like HMAC-SHA256 or HMAC-SHA3.

Q: What are the penalties if PSP's don't comply with the new RTS regulations by Nov 2018?

PSD2 is a European directive that all EU member states need to adopt. Payment Service Providers need to comply with PSD2's requirements in order to be legally recognized as payment service provider with the right to provide services in the EU.

Q: For SMS based authentication, in case 3DS process is used, where an ACS generates the OTP and distributes to the cardholder registered mobile number, do we still need to include the payment details (e.g. beneficiary account number, amount,etc.)?
Our interpretation of the Dynamic Linking requirements in the final draft RTS is indeed that the payment information needs to be included in the SMS message for payment authentication.

Q: With the issue of the ECB Recommendations in Jan. 2013, the ECB published an assessment guide in 2014. Do you expect a similar assessment guide will be issued by EBA on the basis of RTS on SCA and CSC?
We don't have information that confirms or denies that the EBA would issue a similar assessment guide.

Q: To be compliant in 2aa situation, do both apps need to be protected by RASP? or only the authentication app?
The authentication app needs to be protected with RASP. The banking app may be protected, but it is not required in the final draft RTS.

Q: Do you intend to label each token model (e.g. DP310) with a PSD2 compliance indication?
VASCO is not currently planning to do this. Additionally there is no formal certification program for strong authentication solutions under PSD2.

Q: Is DIGIPASS SDK available/compatible with NativeScript?
Yes, this is the case.

Q: Is the VASCO GO 6 DIGIPASS compliant with RTS with regards to the dynamic linking requirement for High Value Payments?
In general, the GO-tokens do not generate authentication codes over payment information (such as the amount of money). For this reason, it cannot be used for Dynamic Linking, which is always required for payments above 500 euro.

Q: Does VASCO have a solution to use the 'inherence' factor (Biometrics) as authentication element?
Yes, DIGIPASS for Apps supports biometric authentication based on fingerprints, face scan, and the behavior of the user.

Q: Is the VASCO solution a cloud-based solution? And if Yes private or public?
IDENTIKEY Risk Manager is available on-premise as well as in the cloud. The cloud version is hosted by VASCO.

Q: Is IDENTIKEY Risk Manager compliant with RTS requirements?

Yes, IDENTIKEY Risk Manager can perform transaction risk analysis according to the requirements in the final draft RTS.

Q: Could you elaborate on the secure communication offered by DIGIPASS for Apps? What is used to secure it? What is required on the server?

The Secure Communications functionality of DIGIPASS for Apps allows creating a secure communication channel between the app and the server, protecting the confidentiality, integrity and authenticity of all payment information. DIGIPASS for Apps comes with both client-side and server-side SDKs to establish the secure channel. In this way PSPs can easily set up a secure channel without having to manage the complexity of the secure channel themselves.

*The site is for informational purposes only and does not provide legal or financial advice,and should not be relied upon in such a manner. Customers are responsible for fully understanding, interpreting and complying with PSD2 regulations.