RSA

SOLUTION BRIEF

PSD2 & THE NEW RULES FOR STRONG CUSTOMER AUTHENTICATION

moviri

On February 23, 2017, the European Banking Authority (EBA) released the Final Report of the Draft Regulatory Technical Standards on Strong Customer Authentication and Common Secure Communication for the Payment Services Directive 2 (PSD2).

This final report heralded a welcome change in the EBA's position on the exemption to Strong Customer Authentication (SCA) based on transaction risk analysis. At first glance, this exemption looks quite tough to qualify for—but fortunately, the RSA® Fraud & Risk Intelligence Suite has operationally been helping its customers prevent fraud in harmony with current EBA expectations.

The major issue facing the financial industry was that the August 2016 Consultation Paper did not allow risk-based SCA. Instead, it defined a limit of 10 euros, beyond which SCA for every transaction was mandatory. In essence, the frictionless customer experience that risk-based authentication provided was in danger of being eliminated. More than 220 responses to the consultation paper helped bring transaction risk analysis back to the final report. The EBA has allowed a new exemption based on transaction risk analysis—and now that the Final Report is out, we can take a closer look at what we have to work with.

Another challenge is represented by the EBA requirements for minimizing the risks of mistaken or fraudulent transactions. PSD2 prescribes several risk-based factors to be taken into account when monitoring transactions, including signs of malware infection. Moviri, a global security consulting company, has demonstrated how these requirements can be effectively put in place by integrating RSA solutions with advanced malware detection based on Cleafy Detect clientless threat detection. The overall solution provides a unified solution that allows customers to both achieve PSD2 compliance and reduce risks.

SCA FACTS

Fundamentally, SCA is intended to secure the end user and help reduce fraud when accessing their account online, and performing payments or other actions online, which can be linked to fraud. Fraud is continuously changing. This includes not only new threats, but the new methods fraudsters are employing, such as leveraging social media to stay in the game. Thus, the financial services industry needs innovative and tested security products to keep fraud in check.

The financial services industry needs innovative and tested security products to keep fraud in check.

SCA is defined by the PSD2 as using at least two elements of knowledge (e.g., PIN/password), possession (e.g., smartphone, hardware token) and inherence (e.g., biometrics). SCA itself also needs to be secure so that its elements:

- cannot be disclosed (i.e., PINs/passwords need to be masked on screen) [Chapter 2, Article 6]
- cannot be replicated (i.e., device data can't be copied to another device)[2, 7]

RSA

- have low false positives (i.e., biometric methods need to perform well)[2, 8]
- are independent (i.e., compromise of one element doesn't compromise the others)[2, 9, 1]

Special attention is required for multipurpose smartphones and tablets to mitigate the risk of device compromise. Separate secure execution environments are required to secure the payment and the strong customer authentication.[2,9,3,a] The EBA doesn't preclude achieving this in a single app combining payments and authentication, or two separate apps, such as an online banking app and a separate authentication app.

Furthermore, the apps need to assess whether the device has been altered or compromised (e.g., jailbreak, rooted, emulator detection capabilities).[2,9,3,b] Special attention is also required to mitigate the risk of malware infection (e.g., MITB, MITM, RAT-in-the-Browser, Mobile Overlay), that is occurring on the end-point side which represents the weakest link in the transaction flow and the most targeted point by fraudsters.

The SCA process needs to confirm to the user the transaction amount and payee during the authentication [2,5,1,a], then create an authentication, code or token specific for the transaction amount and the payee,[2,5,1,b], such that it:

- is resistant to forgery[2,4,2,c]
- does not disclose its source elements[2,4,2,a]
- is used only once[2,4,1]
- cannot be used to generate a new code based on previous codes[2,4,2,b]

When authentication fails, institutions cannot identify which element of knowledge, possession or inherence was incorrect.[2,4,3,a] Multiple authentication failures (maximum of five) result in a temporary or permanent account block; the user needs to be notified of a block and be provided a secure method to reverse the block.[2,4,3,b] User sessions need to time out after five minutes of inactivity.[2,4,3,d]

FIXED EXEMPTIONS FOR SCA

The exemptions for SCA are controversial because of the need to find a balance between security, fraud reduction, innovation, competition, user-friendliness and accessibility, and at the same time, have guidelines that are clear and unambiguous. Across the EU there is a wide range of banking cultures, from existing strong customer authentication to single-factor authentication, low fraud to high fraud, and given the PSD2 also introduces open banking to third parties, this balance becomes more difficult to manage.

The SCA exemptions include a range of fixed rules, including:

- viewing only the balance[3,10,1,a] or last 90 days of transactions [3,10,1,b]
  - first time viewing the balance or transactions requires SCA[3,10,2,a]
  - after 90 days since last SCA, need to authenticate again[3,10,2,b]

RSA

- contactless card transactions less than 50 euros [3,11,a]
  - SCA required again when accumulated contactless transactions value exceeds 150 euros or five transactions[3,11,b]
- card transactions at parking meters and toll gates[3,12]
- payments from and to accounts owned by the same user[3,14]
- payments to a previously created beneficiary[3,13,1,a]
  - creating or changing the beneficiary requires SCA[3,13,2,a]
- series of payments of the same amount to the same beneficiary[3,13,1,b]
  - the first payment, creating or changing the beneficiary requires SCA[3,13,2,b]
- low-value transactions less than 30 euros [3,15,a]
  - SCA required when accumulated transaction value exceeds 100 euros or five transactions[3,15,b]

TRANSACTION RISK ANALYSIS

Beyond the fixed exemptions for SCA, the Final Report provides an exemption based on transaction risk analysis,[3,16,1] allowing for risk-based authentication. However, the EBA has specified transaction thresholds up to 500 euros based on fraud rates where this exemption can apply. This means that the transaction risk analysis solution needs to perform to the specified fraud rates or risk-based authentication cannot be used.[3,16,2,a]

Transaction risk analysis needs, at a minimum, to include the following in the risk assessment:[1,2,3],[1,2,4],[3,16,c]

- abnormal spending behavioral patterns
- payment history of the user and the user population
- location of payer
- location of payee account
- lists of compromised or stolen authentication elements
- payment amount
- known fraud scenarios
- unusual information about the device or software
- signs of malware infection

It is clear to RSA, though, that a transaction risk analysis system needs to provide a lot more than the functions in this list in order to achieve the required fraud rates.

The reference fraud rates are calculated by the total value of the transactions for each payment type over a 90-day history:[3,16,d]

RSA

$$\textit{Reference Fraud Rate \%} = \frac{\textit{Total value of fraudulent successful transactions}}{\textit{Total value of all successful transactions including both SCA and exempted}}$$

Note this is totaling the *value*, not the *number*, of transactions. The reference fraud rates are equivalent to fraud basis points divided by 100.

The reference fraud rates achieved are used to determine up to what threshold the exemption can apply.[3,16,b]

For example, if a bank achieves a fraud rate of three basis points for card-not-present (CNP) transactions, the bank qualifies for a transaction risk analysis exemption for SCA on CNP transactions up to 250 euros.

MONITORING SCA AND FRAUD RATES

A financial institution's SCA methods must be documented, tested and audited by its independent auditor,[1,3,1] including ongoing reporting of the fraud rates, to evaluate compliance to use the exemption for SCA.[3,16,e]

The financial institution's fraud rate reports need to:

- be provided on at least a 90-day basis[3,17,1]
- be separated for each payment instrument[3,17,1]
- include the total value of fraudulent payment transactions[3,17,1,a]
- include the total value of all payment transactions[3,17,1,a]
- contain the observed fraud rates[3,17,1,a]
- contain a breakdown of payment totals with SCA and exempted[3,17,1,a]
- indicate the average transaction value with breakdown of SCA and exempted[3,17,1,b]
- list the number of transactions with exemptions and percentage to total number of transactions.[3,17,1,c]

When the observed fraud rates exceed the reference rates for 180 days, then the transaction risk analysis threshold needs to be lowered, or if below the lowest reference rate, the exemption can no longer be used.[3,18,1] The exemption may be reinstated when the observed fraud rate has been restored below the reference rate for 90 days.[3,18,2]

ADDRESSING PSD2 REQUIREMENTS FOR STRONG CUSTOMER AUTHENTICATION

Investing in an effective fraud risk analysis system is critical to companies seeking to remain competitive and meet global and regional regulations. RSA is focused on building authentication solutions that help customers determine how they can address the requirements of SCA while maintaining a user-friendly experience that minimizes friction for online banking, payments and e-commerce transactions.

RSA

RSA Adaptive Authentication is a risk-based authentication solution that provides detection and visibility into fraud activity across web and mobile channels. It brings together information about behaviors, devices and known fraud to help organizations minimize losses from high-risk transactions.

If additional authentication is required to validate a customer's identity for high-risk transactions, RSA Adaptive Authentication supports a variety of strong customer authentication methods, including biometrics, transaction signing, out-of-band authentication with SMS or push OTP sent to the consumer's mobile device, and more.

RSA Adaptive Authentication goes well beyond authentication at the points of login and transaction. The RSA Risk Engine analyzes more than 100 fraud indicators and assigns a risk score to each transaction in real time. The solution offers a robust set of features and benefits, including:

- **Behavior profiling** compares current behavior to a consumer's typical behavior in making a risk determination. The user profile determines if the various activities are typical for that user or if the behavior is indicative of known fraudulent patterns. Parameters examined include frequency, time of day and type of activity.
- **Policy management** allows organizations to translate risk policies into decisions and actions through the use of a comprehensive rules framework.
- **Device profiling** analyzes the consumer's current device to determine if it has been used by that consumer in the past, whether its IP address is on a blacklist and whether the geolocation is appropriate, among other considerations.
- **Case management** flags high-risk transactions and fraud incidents for review by a fraud investigator. Organizations define which transactions are subject to case management using the rules engine.
- **RSA eFraudNetwork.** The RSA eFraudNetwork is a repository of fraud patterns gleaned from RSA's extensive network of customers, internal research lab, ISPs and third-party contributors across the globe. When a fraud pattern is identified, the fraud data, transaction profile, device fingerprints and payee (mule) account are moved to a shared repository and is one of the many fraud indicators contributing to the Risk Engine. Nearly one in five fraud transactions are identified by the RSA eFraudNetwork at the time of the transaction.
- **Organization-provided intelligence** can be utilized to impact risk scores as well. Through the ecosystem approach, organizations can contribute additional insights from their business, other antifraud tools and third parties to enhance the risk assessment and fraud detection rates.

The integration of RSA Adaptive Authentication with best-of-breed malware detection further improves customer ability to reduce risks, minimize customer friction and improve the operational efficiency in managing security

incidents and cases. Cleafy Detect is the clientless, real-time threat detection technology that complements RSA risk-based authentication capabilities provided by RSA Adaptive Authentication. Cleafy provides unique end-to-end visibility on how malware is compromising web and mobile applications and provides insights on the real customer experience under attack, which can be leveraged to better anticipate and counter fraud campaigns.

The ability to combine RSA Adaptive Authentication and Cleafy Detect into a single, cohesive solution has been proven by Moviri, a global security consulting company and an RSA strategic partner. Moviri has designed a reference architecture for online fraud prevention, which has been implemented by leading European corporate and retail banks to enable multilayer risk analysis (at session, channel, device, user and transaction layer), better support SCA orchestration and address PSD2 compliance requirements.

CONCLUSION

There is a renewed industry interest in digital banking and card solutions being realized with PSD2. To maintain the frictionless customer experience, the financial services industry demanded risk-based transaction analysis in combination with SCA. The EBA has conceded and allowed this in their Final Report. However, it seems at first glance the exemption reference fraud rates are quite restrictive, and the threshold maximum of 500 euros might be considered to be below the risk appetite of some in the industry. The EBA has the opportunity in the future to review and update the fraud rates, if necessary. Transaction risk analysis defined with the thresholds and reference fraud rates does, however, provide what the EBA was tasked to do—provide a level playing field and be legally acceptable.

RSA and Moviri are working together to address the challenges posed by the new PSD2 regulation with a dedicated joint campaign that provides a comprehensive approach to fraud mitigation covering processes, technology and services. RSA also selected Moviri as an official Technology Service Provider (TSP) for Africa, Europe and Turkey for its RSA Adaptive Authentication for eCommerce solution, which enables a risk-based approach to 3D Secure to fulfill with PSD2 requirements for credit card transactions.