

Migration plan of the French community for the gradual implementation of strong customer authentication on online card payments

The second European Payment Services Directive (PSD2)¹, which defines strong customer authentication (SCA), entered into force on 13 January 2018. The related regulatory technical standards on strong customer authentication (RTS SCA&CSC)² will come into force on 14 September 2019 and will require that “a strong customer authentication that should be applied each time a payer accesses its payment account online, initiates an electronic payment transaction or carries out any action through a remote channel which may imply a risk of payment fraud or other abuse” (art. 97 PSD2).

With regard to remotely initiated card payments however, the implementation of regulatory requirements on strong customer authentication starting from 14 September 2019 raises two different types of issues:

- With respect to the card issuing bank / consumer relationship: in its opinion released on 13 June 2018, the European Banking Authority (EBA) stated that entering the details shown on a payment card during an online payment cannot be considered one of the two authentication factors required for the implementation of SCA. Therefore, the main customer authentication solution provided by France’s main banks for online card payments, i.e. entering card details and a one-time password (OTP) received via SMS, can no longer be considered “strong” and therefore is not a SCA solution in accordance with the new regulatory framework.
- Regarding the e-merchants / acquiring and issuing banks / acquiring payment service providers interfaces: data exchanges for online card payments are performed using a community IT infrastructure based on the 3D-Secure protocol. Yet its current implementation (3D-Secure v1, activated by the sole merchant according to his own criteria) does not allow for compliance with some of the rules laid down in PSD2 : the issuing bank does not have the final say on whether its cardholder should authenticate; and some exemption factors from strong authentication (trusted beneficiaries, enriched dialogue regarding transaction risk analysis, etc.) can only be partially managed.

¹ Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market

² Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication

Projects to implement authentication processes compliant with the SCA definition on the one side, as well as to support the migration of all actors (schemes, banks, acquiring payment service providers, merchants) towards 3D-Secure v2 compliant infrastructure on the other side, both require a significant amount of time for their technical implementation, as a result of the strong interdependencies between the various actors of the payment value chain.

In order to meet the RTS SCA&CSC application deadline of 14 September 2019 while nevertheless acknowledging that the market needs time to make the necessary adaptations, the EBA invited national authorities in its opinion issued on 21 June 2019 (EBA-Op-2019-06) to submit a migration plan towards PSD-2 compliant solutions by next fall. In that context, Banque de France, together with the French community under the aegis of the French Observatory for the Security of Means of Payments (hereafter the OSMP or the Observatory), designed a plan seeking to identify the necessary adaptations and pilot their implementation by all the actors involved.

This migration plan, which aims at addressing the issues faced by French actors, is twofold and encompasses:

- i) The deployment of strong customer authentication by issuing banks, as presented in the 2018 annual report of the OSMP, with a view to gradually substitute OTP SMS with more advanced authentication techniques ;
- ii) The technical migration towards 3D-Secure infrastructure for card payments, in order to properly manage responsibilities and exemptions as required by the European regulation.

This migration plan will be closely monitored by a dedicated migration taskforce within the OSMP and chaired by the Banque de France. This group will gather representatives of the various stakeholders implicated in either section of the plan ; it will meet on a monthly basis at least, and will be in charge of i) checking that the main deadlines and targets are met; ii) validating structuring deliverables; iii) identifying potential issues; iv) making recommendations where appropriate.

1. Migration towards strong customer authentication solutions

1.1 Migration plan and monitoring

This section of the migration plan, which was designed under the OSMP's aegis, is intended to pilot the deployment and gradual build-up of new SCA compliant solutions³; the OSMP officially endorsed this plan during June 2019 meeting, and validated its presentation in its 2018 annual report. A statement on the migration progress will be published in the future Observatory's annual reports.

2019	<ul style="list-style-type: none">• June: stocktake• July: publication of the migration plan• 14 September: entry into force of the RTS SCA&CSC• December: update at the Observatory's plenary session
2020	<ul style="list-style-type: none">• January: launch of communication campaigns aimed at e-merchants• February: launch of an initial communication campaign aimed at cardholders• June: first update presented at the Observatory's plenary session• July: publication of the first update• December: update at the Observatory's plenary session
2021	<ul style="list-style-type: none">• June: second update presented at the Observatory's plenary session• July: publication of the second update• September: launch of a second communication campaign aimed at cardholders• December: update at the Observatory's plenary session
2022	<ul style="list-style-type: none">• June: third update presented at the Observatory's plenary session• July: publication of the third update

In order to monitor the progress made by the main banking institutions in carrying out this migration, the Banque de France has developed indicators that will be collected twice a year and will provide the information needed to report on progress on the following aspects:

- the downward trend in the use of non-compliant systems;
- the development of authentication solutions that comply with the new regulation.

The main French banking institutions will report on the indicators shown in the table (inset) and the Banque de France will compile the results. In addition, the OSMP will ensure that payment market players offer solutions that are properly adapted and accessible to all their customers, particularly those whose equipment and consumer habits could impede the use of advanced technologies.

Indicators for online card payments and sensitive online bank transactions

³ The main PSD2 compliant authentication technologies used by French payment service providers were presented at the OSMP; the opinion released by the EBA on 21 June 2019 also included details and concrete examples of such solutions.

a) Online card payments

Monitoring	Indicators
SMS OTP trends	Number of cardholders enrolled in an authentication arrangement when making an online card payment
	Number of cardholders enrolled in a non SCA-compliant authentication arrangement (and not enrolled in a compliant system) when making an online card payment
	Number of online card payments during the past three months
	Number of online card payments during the past three months requiring strong customer authentication in compliance with the regulation
	Number of online card payments during the past three months triggering the use of a non SCA-compliant authentication arrangement
Development of SCA-compliant arrangements	Number of cardholders enrolled in at least one SCA-compliant authentication arrangement when making an online card payment
	Number of online card payments during the past three months triggering the use of an SCA-compliant authentication arrangement

b) Sensitive online bank transactions

Monitoring	Indicators
OTP SMS trends	Number of customers of online banks, or payment initiation or aggregation services enrolled in an authentication arrangement when carrying out sensitive transactions (credit transfer orders, adding account beneficiaries, quarterly renewal of online payment account tokens)
	Number of customers of online banks, or payment initiation or aggregation services enrolled in a non SCA-compliant authentication arrangement (and not enrolled in a compliant system) when carrying out sensitive transactions
	Number of online bank, or payment initiation or aggregation transactions during the past three months
	Number of online bank, or payment initiation or aggregation transactions during the past three months requiring strong customer authentication in compliance with the regulation

	Number of online bank, or payment initiation or aggregation transactions during the past three months triggering the use of a non SCA-compliant authentication arrangement
Development of SCA-compliant arrangements	Number of customers of online banks, or payment initiation or aggregation services enrolled in at least one SCA-compliant authentication arrangement when carrying out sensitive transactions on an online banking site or via an initiation or aggregation service
	Number of online bank, or payment initiation or aggregation transactions during the past three months triggering the use of an SCA-compliant authentication arrangement

1.2 Target migration rate

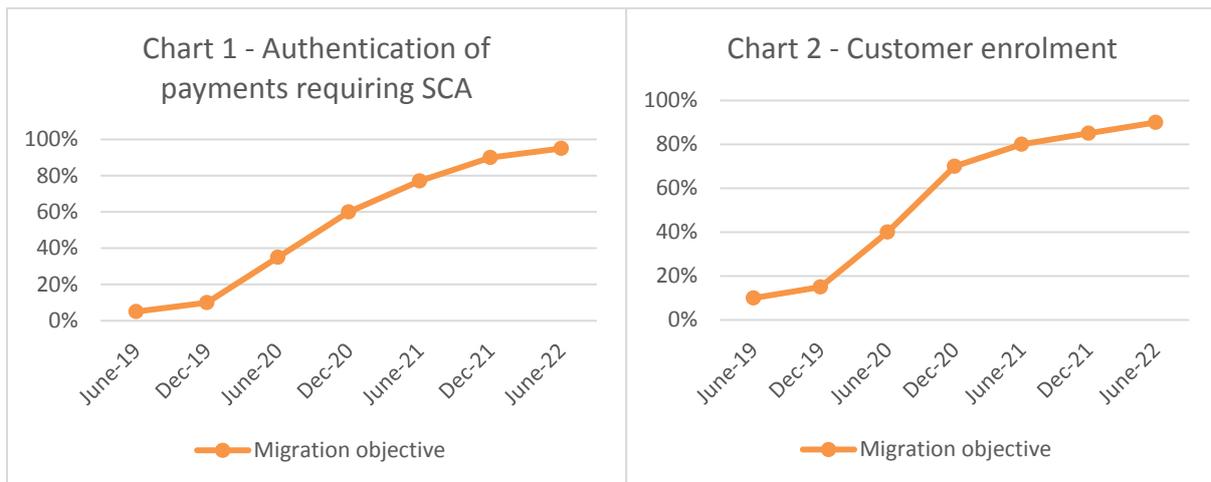
The migration objectives set by the OSMP provide for a two-step approach:

- The primary migration stage, which spans a period of 18 months, should ensure that the vast majority of cardholders is enrolled and authenticated, in particular via solutions based on mobile banking applications. This first migration period should enable to reach more than 75% of users and online transactions ;
- An additional period of up to 18 months, which will be dedicated to finding solutions to get stragglers on board (disadvantaged or ill-equipped people, expatriates, etc).

Charts 1 and 2 present intermediate targets designed to help pilot these migration phases. They will be monitored at pre-defined stages and summary updates of the results will be published by the OSMP.

The following assumptions apply in the development of this extended coverage.

- Customers must be equipped with devices that are compatible with a ramp-up of transactions authenticated using these new methods. However, cardholders that are already equipped, and thus more used to performing online transactions, are subsequently expected to generate more transactions than those who will not yet have migrated, which explains continued sustained growth in 2021 and beyond.
- While the beginning of the migration will be gradual, it will accelerate as a result of operators' communications and the more widespread introduction of the new arrangements to the general public. However, it is expected that once 80% of customers are equipped, the pace of migration will slow down given the greater effort required to get stragglers on board.
- Consequently, the situation will have to be reviewed in June 2021 with regard to the remaining "SMS OTP user customers" in order to determine the best approach to take in light of PSD2 regulatory requirements.



2. Migration towards 3D-Secure infrastructure

2.1. Migration plan

The section of the plan relative to the 3D-Secure technical platform for card payments was elaborated by the French community (banks, schemes, technical providers and e-merchants) in order to meet RTS requirements on SCA. This plan was presented to the Banque de France by the French Banking Association as well as the main schemes operating in France in the summer of 2019, and amended so as to meet the regulating authority's requirements. Built over a period of 18 months, its aim is the gradual phasing-out of non-authenticated transactions which are not subject to an exemption by 2021:

- The first 6 months will represent the running-in phase of the 3D-Secure v2 infrastructure. During this period, banks, card schemes and acquiring payment service providers will gradually connect their systems as well as a limited number of final users (cardholders and merchants) to the infrastructure, so as to start processing transactions and test its end-to-end communication.
- Once the running-in phase is over, the following 12 months will be dedicated to monitoring the ramp-up of the 3D-Secure v2 architecture, and gradually incorporate exemptions management functionalities. During this phase, merchants will be encouraged to migrate their (unsecured or based on 3D-Secure v1) native online sale infrastructure towards the new version of the protocol (3D-Secure v2). In the meantime, card issuers will gradually implement a *soft decline* mechanism, providing for the rejection of non-authorized transactions which are not subject to an exemption as defined in the RTS.

2019

Gradual compliance of the whole ecosystem with the EMV 3D-Secure v2 standard

	<ul style="list-style-type: none"> • July : start of the deployment of EMV 3D-Secure v2 by banks and providers • September 9: delivery of the community infrastructure (not supporting the transaction risk analysis exemption - TRA) • September 14: <ul style="list-style-type: none"> ○ RTS SCA&CSC coming into force ○ Beginning of the e-merchant migration towards EMV 3D-Secure v2 ○ Communication campaigns aimed at e-merchants. ○ Gradual management of exemptions by the banks (except for the TRA) via 3D-Secure v2 so as to perform non-authenticated transactions (so-called <i>frictionless</i> mode) • October : launch by the OSMP of the migration taskforce in view of defining the conditions for the <i>soft decline</i> (gradual rejection in case of non-authenticated transactions which are not properly substantiated, although e-merchants will be able to submit a new, SCA-compliant request) • December : Update at the OSMP's plenary session
2020	<ul style="list-style-type: none"> • April 1st : <ul style="list-style-type: none"> ○ Start of <i>soft decline</i> implementation by issuers, provided this action is validated by the "migration" taskforce, depending on the progress of the deployment of ENV 3D-Secure v2 ○ Deployment of the full version of the infrastructure (with TRA) • June : update at the Observatory's plenary session and in its 2019 report • December : update at the Observatory's plenary session
2021	<ul style="list-style-type: none"> • January : update on the remainder of non-authenticated transactions which are not subject to an exemption • End of March: non-authenticated transactions not subject to an exemption are rejected. E-merchants and transactions should either use the EMV 3D-Secure v2 protocol or consistently request authentication

2.2. Migration monitoring

This migration will be monitored through two types of indicators:

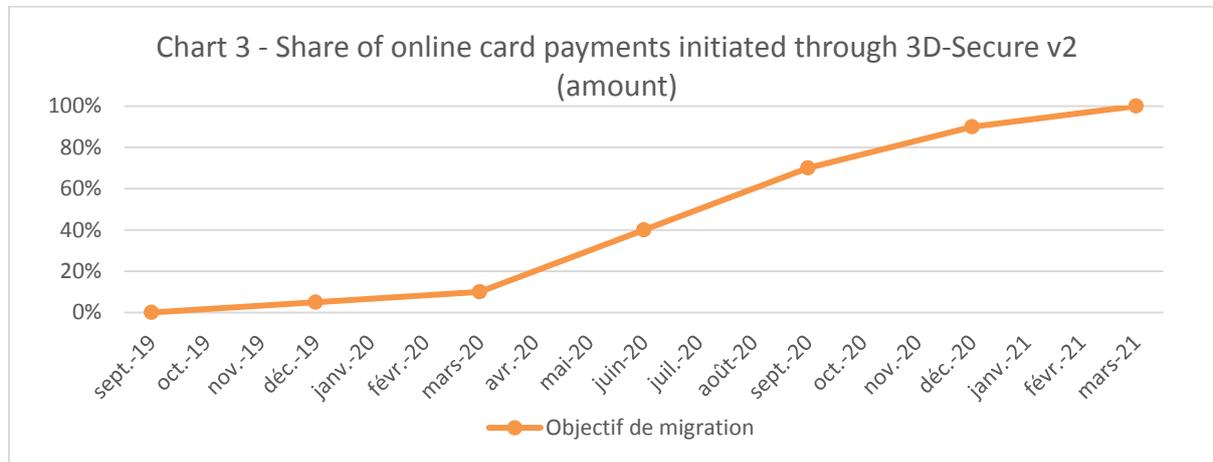
- Deployment indicators, in order to monitor the gradual interconnexion of stakeholders to the 3D-Secure v2 infrastructure (card enrolment, e-merchant equipment) ;
- Operation indicators tracking payment flows and recourse to *soft decline*, in order to monitor the gradual ramp-up of the infrastructure.

Indicators on 3D-Secure infrastructure for card payments	
a) Banks migration towards 3D-Secure v2	
Monitoring	Indicators
Card enrolment on ACS	Number of 3D-Secure v.2 enrolled cards
	Ratio of 3D-Secure v.2 enrolled cards
b) E-merchants migration towards 3D-Secure v2	
Monitoring	Indicators
E-merchant equipment	Number of online sales contracts
	<i>of which unsecured online sales contracts</i>
	<i>of which 3-DSecure v1 contracts</i>
	<i>of which 3-DSecure v2 contracts</i>
Soft decline monitoring	Number of rejected unsecured transactions (<i>soft decline</i> motive)
	Amount of rejected unsecured transactions (<i>soft decline</i> motive)
	Number of approved unsecured transactions
	Amount of approved unsecured transactions
Use of 3D-Secure v2	Number of online transactions using 3D-Secure v2
	Amount of online transactions using 3D-Secure v2
	Number of online transactions
	Amount of online transactions

In addition to collecting migration indicators on the new protocols' deployment, the migration taskforce will monitor issuer and acquirer fraud rates on authenticated and non-authenticated transactions per amount and exemption case, in order to ensure compliance with the thresholds set out in the RTS SCA&CSC. These statistical indicators, which given the fact that they are not tied to the migration are intended to last, will be collected from payment service providers by the Banque de France on a quarterly basis, as set forth in article 21 of the RTS SCA&CSC.

2.3. Target migration rate

The migration objectives shown on chart 3 cover the next 18 months. They will be monitored at pre-defined stages and summary updates of the results will be published.



The following assumptions apply in the development of this extended coverage:

- While the beginning of the migration will be gradual, it will accelerate from March 31 2020 on, as a result of *soft decline* implementation by issuing banks, as soon as EMV 3D-Secure functionalities are effectively deployed by issuers and service providers. Indeed, the last will increasingly reject unsecured online transactions (i.e. without capacity to authenticate the cardholder) on the basis of two criteria:
 - a) Transaction amount exceeding 500€ (which may be lowered later on);
 - b) Merchant identified as displaying enduring high fraud rates, or registering a significant increase of its fraud rate.The OSMP's "migration" taskforce shall clarify these criteria later on. However, it is expected that once 90% of e-merchants are equipped with 3D-Secure v2, the pace of migration will slow down as a result of the greater effort required to get stragglers on board.
- Consequently, the situation will have to be reviewed in January 2021 with regard to the remaining transactions which are not authenticated while not qualifying for an exemption, in order to determine the best approach to take in light of PSD2 regulatory requirements.
- The taskforce shall take into account the degree of complexity required to complete a payment in some specific sectors.