Attendees

Jonathan Grossar (Mastercard)
Rouslan Solomakhin (Google)
Jalpesh Chitalia (Visa)
Lawrence Cheng (Barclays)
Tomasz Blachowicz (Mastercard)
Dean Ezra (Barclays)
Swapnil Deshmukh (Certus Cybersecurity Solutions)

Minutes

Jonathan: we will start with flow “new user – first time purchase on new device”

Jalpesh: today is a recap of high level add card flow and repeat user flow. There were few questions at last meeting how identity works from payment handler perspective, and how does it work when going to another device.
First flow is about adding a new card, customer has never added a card before, has never used SRC before. They go to merchant web site, they select the trigger that initiate PR with appropriate method, browser forwards PR to payment handler with merchant payment request data. In step 5, there are optionalities in terms of what payment handlers do – they can either create a user identity based on device that could be driven by cookies or something else, or based on user credential (they can ask user to create user credential e.g. email or phone number). Then card entry is managed by payment handler – user key enters the card. On step 9, the SRC APIs are being called by payment handler to appropriate SRC system (depending on the card that has been entered). SRC system will go through risk rules and merchant preferences – if a step up occurs on step 10, payment handler may have user interaction with customer. On step 11, payment handler will go back to SRC system and provide step up response gathered from customer. Step 12: SRC system creates payload that includes card references and payment data that is necessary for payment handler to pass to merchant via browser.

Lawrence: on step 6, is it username and password?

Jalpesh: this is entirely left to payment handler – e.g. payment handler may decide to create email address or phone number.

Lawrence: in step 9, card info is 16 digit card, and identity info is user identity?

Jalpesh: it could be either, or, both – i.e. it can be 5, 6 or 5 + 6, depending on what the payment handler has and wants to share with SRC system

Lawrence: when you say step up it is to ensure that card belongs to the person but not a payment authentication?

Jalpesh: this is in context of purchase flow, consumer selects to pay – and creates user credentials. There may or may not be a step up.

Lawrence: step 12, digital card reference is network token?

Jalpesh: payment data is the scheme token, card reference is metadata of the card

Jonathan: i.e. 4 last digits and card art.

Lawrence: ok, so payment data is the token which is being returned. Easy to understand- not very different from other payment apps- step up is 3DS, trigger response is tokenization etc. So what is the unique thing of SRC outside of 3DS and tokenization.

Jalpesh: unique thing is common payment method across card brands, and it simplifies/abstracts a few things for merchants and payment handler

Jonathan: e.g. one identity for all schemes.

Lawrence: is the benefit of SRC to help acquirers?

Jalpesh: when 'merchant' was mentioned, it is indeed not necessarily merchant, it can be PSP or gateway i.e. whoever is collecting card information from customer. It could be a PSP or Acquirer that initiates step 3 of PR. Benefit to your point is for them to invoke SRC with right parameters and not to have to collect card information, and rely on the browser for a better repeat purchase UX and also standardized UX.

Lawrence: but step 8 is collecting card information?

Jalpesh: yes but it is done by payment handler not by PSP. One payment handler on that device or for that user works across all merchant acceptance.

Lawrence: maybe not question for today, but we need to go through all added values and cost effectiveness for merchants, so that merchants will see benefits and be more comfortable to make the updates. For merchant adoption, merchants need to see value added.

Swapnil: question on step 8- when someone is entering card info, are we pushing to have a secure communication protocol, is there a flow that explains how this is invoked? And how you are encrypting information between steps 8 and 9 as it seems to be the weakest link.

Jalpesh: I can answer the second part of the question. At highest level, payment handler is coding against SRC system specs and those specs will have information on how to encrypt and there is a key exchange between payment handler and SRC systems. If there is a Visa card, Visa keys are used to encrypt, if it is a Mastercard card, Mastercard keys are used to encrypt, by the payment handler. It is in the SRC system specs and will be also in each of the SRC system implementation specs.

Tomasz: I can also add that payment handler is a web component, so it is also assumed that this web component will manage its own UI to collect the card, so on step 8 the consumer will key enter the card info in the web UI of the payment handler, and payment handler will communicate this with SRC systems.

Swapnil: considering that payment handler will manage card info, do you have documentation how key ceremony will happen in the first place? Do you have a process in place.

Jalpesh: yes but it is implementation details. It is not different from a PayPal payment handler, and what happens between PayPal front end and PayPal back end. SRC System or payment method provider generally has to create a solution for it between their front end and backend systems.

Jonathan: we go to second flow “repeat purchase, existing user on same device”

Jalpesh: consumer went purchasing on this device and comes back on this device and uses a trigger from merchant perspective – and merchant or PSP initiates PR and browser forwards PR to payment handler, presumably same payment handler. Payment handler identifies the device if based on device identity (option 1), or on user identity (option 2) – if on user identity it will work with user to establish that it is same consumer. The intent is that payment handler will show a list of cards. The list of cards is asynchronously called by payment handler on each SRC system – so for same user identity even if user has only one visa card, the payment handler will also go to all SRC systems, and say that Mastercard has also cards for same identity then list of cards will come from all SRC systems that are participating with that payment handler. So if a consumer has both a Visa and Mastercard they will both show up on step 9. Consumer selects card and if it is a Mastercard selected, payment handler in step 11 makes a request to Mastercard for checkout request. It is same data as provided in initial checkout request in previous flow, there is also risk decision and possibly step up. Step 14 is response back from SRC systems to payment handler that gets forwarded to the merchant via the browser.

Lawrence: question on steps 7 and 8- if user has added a Citi Mastercard previously – when we say list of cards, consumer will see only one card i.e. Mastercard, so what other cards the consumer could see and why?

Jonathan: consumer will see list of cards coming from all SRC systems that have a card against that same identity, i.e. all cards that have been added in the past to SRC systems against that identity. So if a Visa Chase card has
been added at another moment to Visa SRC system, both the Citi Mastercard and Visa Chase cards will show up in the list of cards in the payment handler.

Lawrence: OK so user has added both cards into the payment handler and therefore both cards are returned.

Jonathan: cards are retrieved from SRC systems, it does not mean it has been added to that particular payment handler.

Jalpesh: from a standard perspective, W3C and SRC, SRC specs talk about ID exchange across SRC systems. If there is an ID Token created by an SRC system say Mastercard, that same identity can be used by the same payment handler to go and fetch card from other SRC systems if they have a card (if they don’t there is nothing coming out of them). This is only possible if the other SRC systems have the same identity – it is subjective as we don’t know what that identity could be – e.g. if payment handler is doing device identity the likelihood to find a card in SRC system is close to none, if they use user identity say email address then Visa may have something for that email address because another bank or payment handler may have sent something to Visa on the same email address.

Lawrence: on the diagram payment handler is responsible for user credentials, which we call user identity, so that user identity is specific to that payment handler, so not sure how SRC systems would be able to map that specific identity to a wider set of cards.

Jonathan: if it is an email then SRC systems may have cards which are not related to a specific payment handler but to the email provided.

Lawrence: but anyone can use my email address – so if someone provides my email address they will get access to my cards?

Jonathan: we may verify the user before they access the card

Jalpesh: there are 2 questions: is that payment handler specific? It depends on the identity type – if it is device ID it is unique to payment handler so the probably to get other cards is close to none, if it is an open identity like phone number you can get other cards if SRC systems recognize it.

Jonathan: I believe the question is also how to prevent unauthorized user to access to list of cards. That user would not necessarily be able to use a card for payment since consumer authentication may be required, but even to access list of cards, there may be verification of the user.

Tomasz: yes step 6 includes user verification of user credentials – e.g. sending a verification link to email address. Rather than asking for password we could send OTP.

Jonathan: if user is recognized on the same device, there may be no need to verify the user to give access to cards.

Jalpesh: step 6 is where payment hander recognized consumer – how the payment handler recognizes consumer, as Tomasz says, the OTP is one of the verification method that SRC systems will trust. As long as the RSC system can trust the assertion that payment handler provided, that this is an email address, then SRC system, depending on that assertion and possibly risk rules they may provide the cards, however they may also decide to step up before giving access to list of cards. Between step 6 and 12 there is a lot of control that systems have.

Lawrence: user expects to see cards they have added to the payment handler. User would be shocked to see as a sudden all the card that appear – do we have customer research showing that user will be comfortable to see all their cards?

Jalpesh: Yes, EMV has done the consumer research, Visa has also done research and perhaps other card brands as well. How is privacy handled: by payment handler or SRC systems, it goes beyond payment flows. If I take just an example: Google Pay, if I add a card to Google Pay then I add another card to the Play Store, that card will also appear in Google Pay.

Jonathan: why user would be shocked?

Lawrence: let's take PayPal: a consumer adds a card to PayPal, then 2 days later you come back and you see a bunch of cards as a sudden when you use PayPal.

Jonathan: it is not a buy with PayPal but a buy with SRC where cards can have been added to different SRC systems.

Tomasz: from SRC perspective, consumer is not interacting with payment handler as a brand- consumer is interacting with SRC systems. If consumer pays with that payment handler on that browser or through other means, consumer will expect to see all cards.

Adrian: might be confusing for 3rd party payment handlers heavily branded with payment handler, unless there will only be one payment handler called SRC payment handler.

Jalpesh: There are two separate questions being discussed: we are talking about consumer comprehension and consumer disclosures. It's best for us to look at EMV Specs that detail the consumer interaction and, to an extent, branding and usability requirements for SRC participants including SRCI and DCF.

Lawrence: merchant adoption and consumer adoption are very important – we must pay attention to consumer perception to ensure that average consumer understands what is happening. Not sure how we can do that, maybe at TPAC to deep dive a bit further.

Jalpesh: from consumer education, branding, disclosure- SRC will have a solution as a payment method with / without W3C. All of that will be consistent with the EMV specs.

Jonathan: we are on the 3rd flow: existing user but user decides to change their device, 3.1 flow.

Jalpesh: on 3.1, assumption is that payment handler only uses device identity not user identity – so when going on a new device, payment handler does not recognize the user and will ask to key enter the card again on steps 6 and 7, it looks like an add card flow, similar to add card the 1st time.

Jonathan: on 3.2, it is user identity that is used, like email.

Jalpesh: in this case, on step 5 there will be user recognition and the list of cards will be displayed. Then on steps 9 and onwards it is not different from the flow #2.

Jonathan: suggestion in step 5 to use the same terminology as in previous flows i.e. 'user credentials'.

Jalpesh: ok will update the flow. (Action Jalpesh to update)

Lawrence: on 3.2 it is not different from Amazon right? It is one-click payment.

Jalpesh: you have to be recognized by the payment handler before cards can be displayed.

Lawrence: I thought that straightforward scenario is to have username password to recognize individuals when going to a new device.

Jonathan: not necessarily as a password may not have established – e.g. an email address used as user identity (verification is done via OTP to that email address).

Tomasz: this is one way of doing this, in future there may be other ways. It is up to the SRC system to accept the form of user credential verification.

Jonathan: we don’t have enough time to cover the 3DS flows – we should go through them in our next meeting. For TPAC, proposal could be to go through finalized flows and have a demo allowing the visualization of the data exchange between merchant and Payment Handler invoked via PR API.