RCS and Payments

Discussing RCS as a payments channel and its potential under PSD2 Strong Customer Authentication

February 2020

About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

For more information, please visit the GSMA corporate website at www.gsma.com. Follow the GSMA on Twitter: @GSMA.

About Consult Hyperion

Consult Hyperion is an independent strategic and technical consultancy, based in the UK and US, specialising in secure electronic transactions. With over 30 years' experience, we help organisations around the world exploit new technologies to secure electronic payments and identity transaction services. From mobile payments and chip & PIN, to contactless ticketing and smart identity cards, we deliver value to our clients by supporting them in delivering their strategy. We offer advisory services and technical consultancy using a practical approach and expert knowledge of relevant technologies. Hyperlab, our in-house software development and testing team, further supports our globally recognised expertise at every step in the electronic transaction value chain, from authentication, access and networks, to databases and applications.

For more information contact pressoffice@chyp.com

ABSTRACT

Rich Communication Service (RCS) was first defined around 2007/8 and was taken on by GSMA as the protocol to replace Short Message Service (SMS). RCS required both software and carrier network upgrades, and initially, there was little appetite for adoption, but this is now changing.

While RCS offers more features than improved security over SMS, the focus of this paper is exploring how RCS might address some of the issues with authentication today. Authentication for consumers using online services has been enhanced over time from basic (username and password) to two-factor authentication (2FA), which is most commonly achieved using one-time passwords (OTP).

Traditionally, OTP has been implemented on mobile devices using SMS, which has not changed much since it was rolled out in the 1990s and has known weaknesses. Despite this, OTP-over-SMS is widely used as an additional factor of authentication, especially in banking. In general, mobile business messages need to be better secured.

RCS offers a better experience and additional features compared to SMS. We have already seen operators in Europe, US and Asia using RCS for increased customer engagement over business messaging campaigns. Google is promoting RCS and launching directly in some markets (e.g. the UK, France and Spain). Adoption is growing quickly, though Apple does not currently support RCS, so market penetration by region will depend upon iOS market share.

Meanwhile, for online payments solutions, the European Union’s Second Payment Services Directive (PSD2) requires banks to apply strong customer authentication (SCA) for electronic payments. Although OTP over SMS is a permitted authentication factor, something better is needed and RCS looks like a likely candidate.

This paper explores how features of RCS can be used to achieve SCA replacing OTP-over-SMS and in particular for online payment applications. The paper then moves further to evaluate different ways that payments can be integrated into RCS directly, offering a complete user journey within the messaging client. It concludes with analysing how RCS can enhance existing payment methods. This is an effort to make consumers, card issuers, and banks aware of the benefits that could be achieved through the use of RCS.

Table of Contents

1. Introduction

1.1 Background and objectives

While RCS offers more features than just improved security over SMS, the focus of this paper is exploring how RCS might address some of the issues with authentication today. Authentication for customers using online services has been enhanced over time from basic (username and password) to two-factor authentication (2FA) which is most commonly achieved using one-time passwords (OTP) and basic identity information (e.g. memorable information).

Traditionally, OTP has been implemented on mobile devices using SMS which has not changed much since it was rolled out in the 1990s and has known weaknesses. Despite this, OTP-over-SMS is widely used as an additional factor of authentication, especially in banking, mainly because it is pervasive because of mobile phone penetration and due to the lack of anything better. In general, mobile business messages need to be better secured.

Meanwhile, for electronic payments solutions, PSD2 requires strong customer authentication (SCA) for online payments. Although OTP-over-SMS is an implicitly permitted possession factor, something better is needed and RCS looks like a likely candidate.

This paper explores how features of RCS can be used to achieve SCA replacing OTP-over-SMS and in particular for online payment applications.

We discuss security risks in using SMS as a channel to deliver OTP. The paper outlines the benefits of RCS as a channel for authentication and how MNOs and the payments sector could benefit from it. We also discuss how payments can be implemented using RCS in conversational commerce (Sections 4 and 5).

1.2 What is RCS?

Rich Communication Services (RCS) enables the next generation of mobile communications. RCS was originally proposed in 2007, and since 2008 the GSMA has been defining the specifications that handset OEMs and MNOs must adhere to, most notably the Universal Profile[1] [1]. The Universal Profile ensures that RCS is implemented as a standard service, and every mobile consumer worldwide can send and receive feature-rich messages in a device and operator agnostic manner. RCS penetration worldwide has been steadily growing with adoption by over 20 device OEMs, platform providers such as Samsung and Google, and more than 50 MNOs worldwide.

RCS is an innovation in Application-to-Person (A2P) messaging and the advanced features that it supports give MNOs and brands a powerful digital marketing tool with high Return on Investment (ROI). RCS features can potentially disrupt the traditional app development and deployment models where a service provider develops separate apps, for instance, one for managing core business, another for rewards and loyalty, another for marketing campaigns and so on.

The MNO business model is based on secure identity provisioned using a SIM and high availability of messaging and calls. SMS has been the most trusted communication method for consumers, and it is widely available. RCS is powered by the MNO technology and built on the SMS model which means other parties, such as banks, can tap into the established consumer base rapidly to explore potential revenue, reduce costs, and provide high quality and secure services to the consumer.

In comparison with SMS, RCS offers feature-rich messaging, supports file transfer, chat, location-based services, and audio/video messaging. The consumer does not need to install an RCS client separately as it is supported natively in the mobile operating system (OS).

1.3 What is PSD2?

The European Union's Second Payment Services Directive (PSD2) [2] mandates several different requirements on authorised Payment Services Providers (PSPs). PSPs are typically – but not always – banks. Although there are many requirements in PSD2 there are two high-level mandates, which have attracted the majority of attention.

The first of these is a requirement for all banks to develop Open APIs to allow access to accountholder data and to initiate payments on an account holder's account. The latter API allows an account holder to push a payment to a recipient, such as an online retailer, without having to pass over their payment details.

The second main requirement is that all electronic payments must be subject to Strong Customer Authentication (SCA). SCA is two-factor authentication where the factors must be any two out of the categories: possession, knowledge and inherence (biometrics). Under PSD2 OTP-over-SMS is permitted only as a possession factor, signalling possession of the SIM.

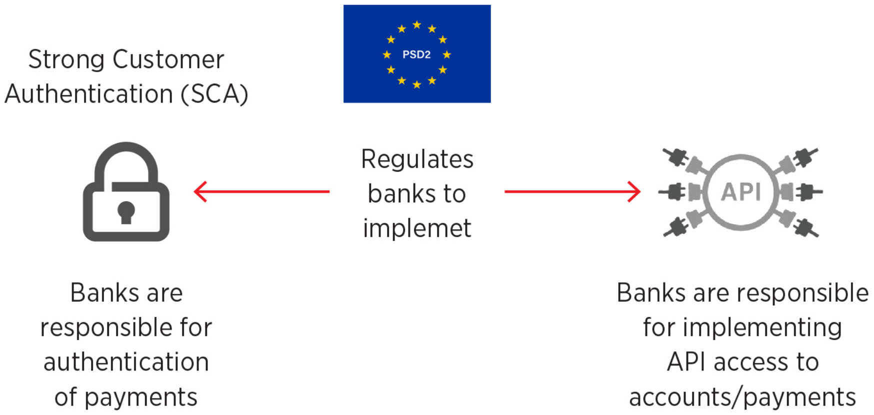
Strong Customer Authentication (SCA)
PSD2
Regulates banks to implemet
API
Banks are responsible for authentication of payments
Banks are responsible for implementing API access to accounts/payments

Figure 1: Strong Customer Authentication under PSD2

SCA applies to all electronic access to an account including API access, card payments, account login and any other interaction with the account which implies risk to the accountholder. Applying SCA to online payments – particularly card payments – introduces significant friction in the payments process and may lead to increased levels of transaction abandonment. There is a high need to find easy, frictionless and secure methods of performing SCA.

2. Strong Customer Authentication

As has been mentioned, mobile business messages need to be better secured. In particular, PSD2 requires SCA for all electronic payments, including online payments. This section explores the PSD2 requirements for SCA and the authentication methods that are currently available to meet them.

2.1 Requirements for SCA in PSD2

ASPSPs – usually, but not always a bank – are responsible for authenticating their consumers, i.e. enforcing SCA, in order to safeguard payment transactions from potential fraud. SCA enables an ASPSP to verify the identity and authenticate the consumer who is using a payment service. SCA also enables the ASPSP to establish if the payment instrument used in a transaction is valid.

SCA requires the use of at least two from the following elements:

- **Knowledge** - something that the consumer knows
- **Possession** - something that the consumer has
- **Inherence** - something that the consumer is (typically using a biometric)

SCA must be applied when a consumer initiates a payment transaction, or accesses their payment account online, or is involved in any activity across a remote channel (e.g. Internet) that can imply risk or fraud, for example, changing a whitelist/trusted beneficiary.

The requirements for SCA and communication are defined in the Regulatory Technical Standards[1] (RTS) document for Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (see Appendix). Appendix A.1 details the most relevant requirements based on RTS and the European Banking Authority's opinion for SCA in PSD2.

The EBA has commented [3] on the elements of SCA and on authentication methods, whether those implemented are SCA or not. The relevant points in the EBA comments are as follows:

- All **elements** must be **independent** of each other, i.e. any security breach of one does not compromise the reliability of the other elements
- The **Knowledge** element should be known only to the consumer and must exist prior to initiation of any payment or account access
- The **OTP** itself is **not** considered as a **Knowledge** element
- OTP or the SMS by itself are not considered as any authentication element. OTP in SMS provides evidence for consumer possessing a SIM card. This card is considered as the **Possession** element and must be associated with the mobile telephone number (MSISDN[2]) to which the OTP was sent by the service provider. We think this will be the case when SMS is Class 2 type which is handled by the SIM

[1] https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2

[2] Mobile Station International Subscriber Directory Number

- The **Possession** element is something only the consumer possesses, e.g. their mobile phone or SIM card
- An OTP received on a device or generated by a hardware device or a software constitutes as evidence of **possession** of the device or software
- ASPSPs shall adopt countermeasures to the risk that elements of **possession** are used by any unauthorised parties

RTS also discusses requirements for Common and Secure Communication (CSC). A.2 details the requirements on communication channels in PSD2. The most relevant requirements are as follows:

- **Device identification**: Payment service providers must ensure secure identification of the payer's device and the payee's acceptance device for electronic payments including but not limited to payment terminals, and also mitigate any risks arising from misdirection of communication to unauthorised parties
- **Traceability**: Payment service providers must ensure all payment transactions and other interactions with consumer including merchants are traceable
- **Secure communication session**: ASPSPs and TPPs must ensure that data exchange via Internet is secured to safeguard confidentiality and integrity using strong and widely recognised encryption techniques

2.2 Authentication methods to meet SCA requirements

ASPSPs have for years been offering their services to consumers across various channels, brick and mortar, telephone, Internet and mobile. Over time, consumers have become 'tech savvy' and have fast adopted the 'connected app' culture. Even before the advent of PSD2 it has become challenging for ASPSPs to roll out authentication methods that cover a wide range of consumer profiles accessing banking and payment services across fragmented technology platforms and market places.

We can consider the typical identification, authentication and authorisation process as a tiered model, with each stage required before the next one can be accessed:

- **Identification**: The process of identifying someone or something to be genuine. For example, a number or username provided by a user that is in the list of authorised users
- **Authentication**: The process of determining whether someone or something is, in fact, who or what it declares itself to be. For example, check if user's credentials match in a database of authorised users
- **Authorisation**: The process of giving someone permission to do or have something. For example, an authenticated user can access certain file directory on a server

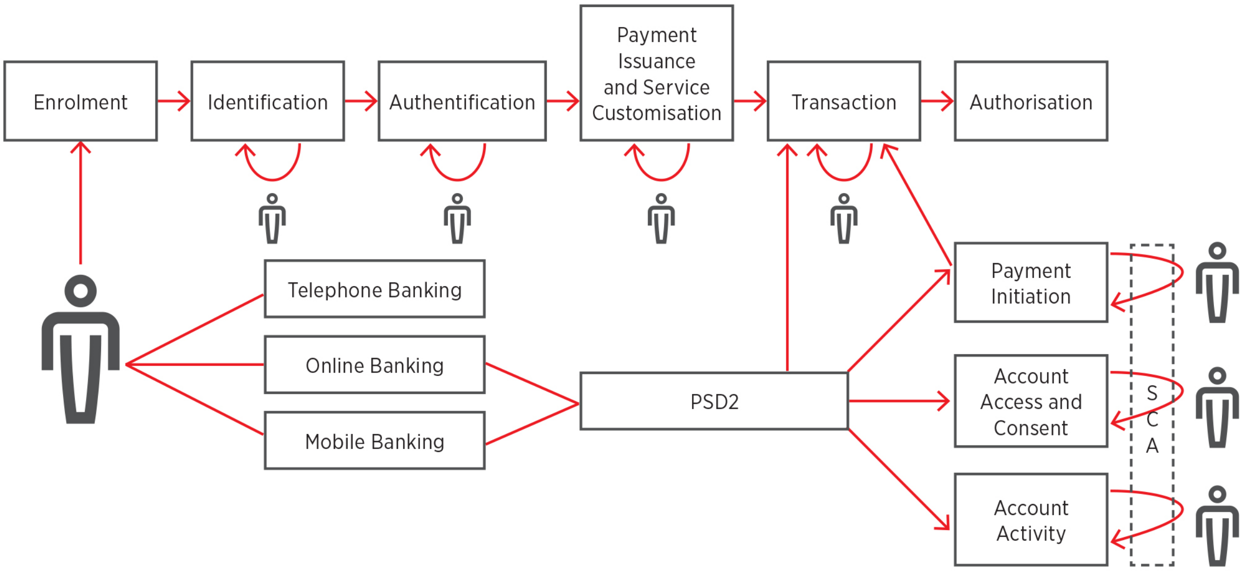

Figure 2: Digital Journey of a Consumer in Banking and PSD2

The typical digital journey of a consumer in banking is fast evolving with PSD2 (see figure 2). The customer icon is used to show which processes involved interaction with the customer.

The process starts with enrolment. Know Your Customer (KYC) processes are critical in banking, and it is required to meet Anti-Money-Laundering (AML) regulations. Identification for the purposes of enrolment is the first step. This is fulfilled in person or remotely by the consumer providing personal information, proof of address, and a valid government-issued ID. The KYC process can be complex and may need additional checks such as checks with credit reference agencies, checks with the birth registry, and so on.

For the second stage, authentication, banks originally introduced basic authentication involving username, password, mother's maiden name, etc., which were not inherently secure. Consumers cannot be expected to choose complex passwords and memorise them so as not to disclose them knowingly or unknowingly. This opened-up security weakness that compromised the authentication process.

The initial evolution from basic authentication was to adopt an additional factor such as memorable secret, or use an OTP received in SMS/email or generated from a device or software; or by using biometrics such as a fingerprint. Next, we witnessed a big growth in two-factor authentication (2FA) and subsequently, multi-factor authentication (MFA). There is government[1],[2] and industry guidance[3],[4] on implementing 2FA. However, this needs careful consideration around cost and device profiles that are supported in the consumer base.

More recently, the consumer authentication processes were further strengthened by using device authentication and fingerprinting combined with risk analysis. Security protocols and advanced technologies such as EMVCo 3-D Secure[3], Public Key Infrastructure (PKI), FIDO Universal

[3] 3DS process involves device/browser fingerprinting, Cardholder authentication and risk analysis. In 3DS, the authentication step ensures that it is the Cardholder who is performing the transaction. More information is available in https://www.emvco.com/emv-technologies/3d-secure/

Authentication Framework (UAF), and behaviour profiling were added to build a comprehensive list of risk-based authentication options.

2.2.1 Authentication Methods

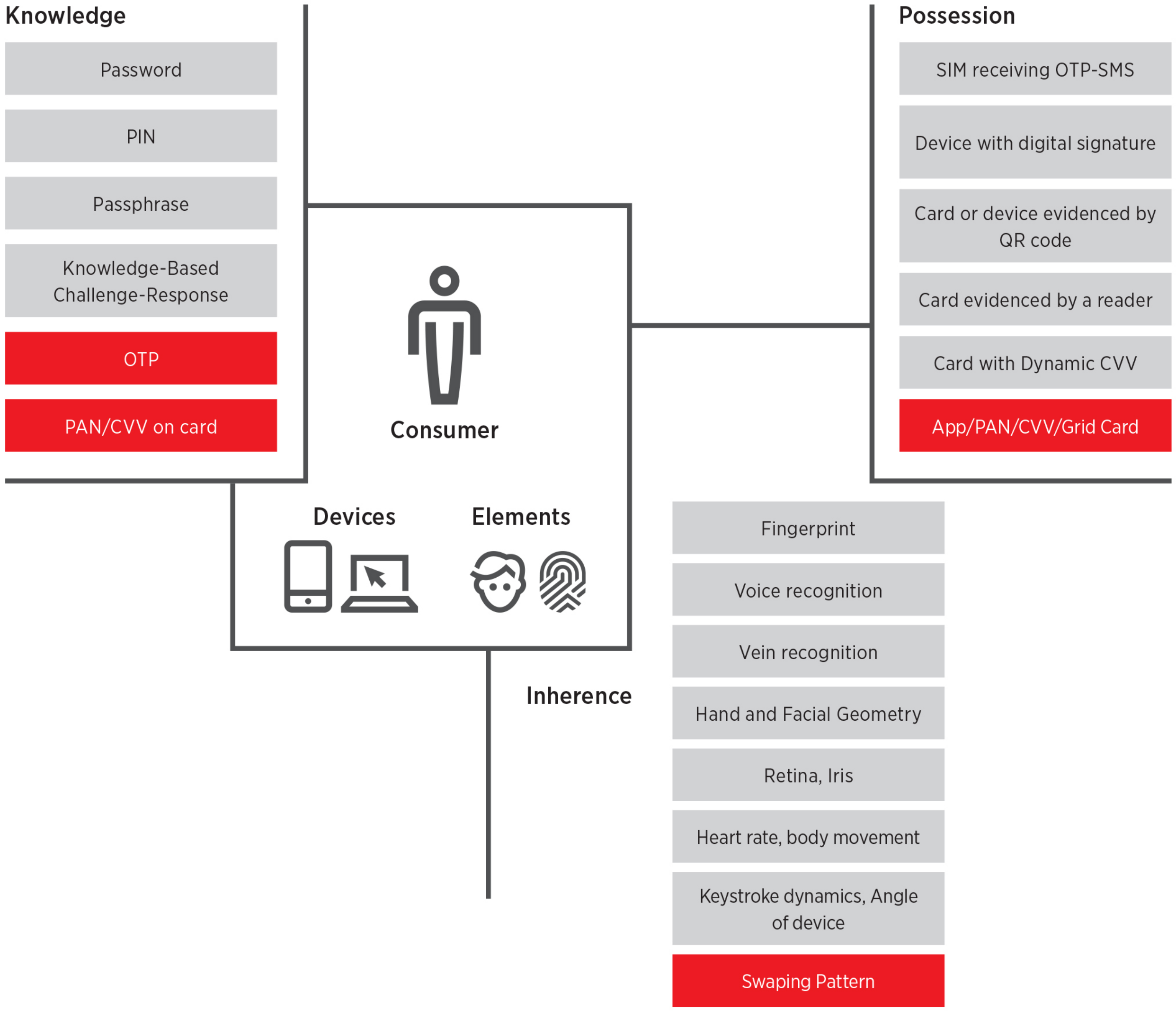

Figure 3: A non-exhaustive list of authentication methods available for APSPs to meet PSD2 SCA requirements

Proliferation of mobile devices and associated technologies, increased connectivity and with consumers having mobile device profiles has led to the success of OTP over SMS and the introduction of fingerprint- based biometrics as common additional factors of authentication. However, there is no silver bullet for authentication that can cover all consumer profiles, and when it comes to SCA banks need to consider a range of authentication methods to suit different account holder profiles.

Figure 3 shows a non-exhaustive list of authentication methods available for banks to meet SCA requirements under PSD2. It depicts several methods that either conform (in blue) or do not conform (in red) to PSD2 according to the EBA[4]. OTP delivered over SMS is widely used for 2FA.

[4] https://eba.europa.eu/eba-publishes-an-opinion-on-the-elements-of-strong-customer-authentication-under-psd2

This approach may be preferred for several reasons. It enables fast deployment to the consumers, and it involves low cost as authentication can work OTT, most of the consumers use a mobile phone and banks do not need to issue them. However, the SMS channel has known inherent security weaknesses which we discuss in the next section.

2.2.2 SMS as a channel to deliver OTP

According to a NIST report[5] SMS as a channel for delivery of authentication secrets such as OTP was originally “deprecated”. However, it was later clarified that SMS channel is “restricted” for government use allowing organizations to use SMS as long as they have adequate mitigation in place against any known risks. We summarise a few common risks here. More details can be found in the Appendix.

- **Fraudulent SIM replacement**: In this scenario, fraudsters can take over a victim’s mobile subscription by using unauthorised number porting or ordering a replacement SIM. Fraudsters can use social engineering techniques to achieve this. Having successfully taken over the victim’s account, fraudsters can receive the OTP-SMS required to complete a legitimate transaction. The victim may become aware of this attack only when they notice their SIM is inactive and is unable to make or receive calls and messages. This attack is also known as SIM-Swap or SIM-Jacking

- **SMS re-routing**: Attackers can exploit vulnerabilities in SS7 and potentially re-route and access SMS messages containing OTPs and which can be used to complete a payment transaction

- **Malware**: Fraudsters can exploit malware installed on a victim’s mobile phone and retrieve OTPs from SMSs to complete a payment transaction

- **Phishing**: Fraudsters can become a Man-In-The-Middle between the victim and a legitimate service provider. The victim may be redirected to a fake website via a phishing message, and the fraudster can readily capture basic authentication information from the victim. The victim may also be convinced unwittingly to supply OTP information

- **Lack of confidentiality**: SMSs are stored as plaintext in the Short Message Service Centre (SMSC) before delivery to the intended recipient. Any security compromise of the mobile network including the SMSC due to malware or insider attacks can lead to potential disclosure of OTPs in SMSs

- **Delayed delivery**: An SMS containing an OTP may not be delivered in a timely manner due to network congestion. This is more common in locations with unusually high numbers of mobile users

- **Delayed presentation to consumer**: If memory is low in the mobile phone the SMS with OTP may not be available to the consumer in a timely manner

2.2.3 Alternatives to SMS to deliver OTP

MNOs may apply tight controls to combat SIM-swap, unauthorised number porting, and patching SS7 weaknesses. These include monitoring for unusual consumer activity and call centre

[5] https://pages.nist.gov/800-63-3/sp800-63b.html

operations. However, those controls do not seem to be practical. From the recent news reports it appears that attackers are using social engineering techniques on MNO staff and unwitting consumers, and still managing to get hold of secrets delivered over the SMS channel. However, most of the alternatives to OTP-over-SMS are not appealing.

Alternative method	Description
OTP over a voice call	Consumer receives a voice call with OTP and then completes the transaction.
OTP over Push Notifications	Consumer registers his/her mobile phone to receive push notification service. The registration step links a dedicated app to the service. The app receives push notifications from the service about pending OTP, which is then retrieved over adequately secured REST API. Consumer then uses this OTP to complete a transaction.
OTP generated from software	Another approach is generating OTP using a software authenticator app which uses a shared cryptographic key with the service provider. The consumer supplies the generated OTP to the service provider during sign-in process which is then validated to grant/deny access. An example of such software authenticator is Google Authenticator.
OTP delivered over RCS	This approach is using RCS messaging channel to deliver OTP to the consumer. Consumer can then stay within RCS context and complete a transaction that requires OTP or switch context to utilise the OTP.

Table 1 Alternative methods to OTP-over-SMS

Considering the SCA and CSC requirements in PSD2, it seems the most attractive alternative to the SMS channel may lie with RCS messaging. We explore whether RCS is a suitable channel to deliver an SCA factor in Section 3.

3. Exploring RCS as a channel

3.1 Key differences between SMS and RCS

SMS messaging functions are typically a part of the wider MNO infrastructure which includes signalling, authentication, billing, data and value-added services. SMS channel also requires inter-working with other MNO infrastructures to fulfil end-to-end message delivery. The routing functions of SMSs are based on SS7 which has its own security issues that we have highlighted in the previous section.

RCS, on the other hand, is IP based, as we highlighted in Section 1, and the infrastructure mainly comprises of an IMS core with designated Application Server (AS) functions. The messaging feature in RCS is enhanced by RCS Business Messaging (RBM) supported by backend platform components. For inter-working with other MNOs and third-party infrastructure, RBM platform APIs are made available for any aggregators to consume.

Brands, including service providers such as banks, need to reach their consumers for provisioning and maintaining services, marketing and promotions, fulfilling security functions and providing alerts, and importantly, for customer support. This A2P model has been, typically, based on the SMS channel which has a broad reach to the consumer base. It is a complex undertaking for service providers to manage A2P by themselves, i.e. directly engage with MNOs, and they often choose to commercially engage with intermediaries with appropriate service level agreements. These intermediaries include messaging aggregators who have agreements with multiple MNOs to ensure global reach.

Shifting from SMS to RBM will not be much different for service providers from the existing SMS business model. Service providers can utilise any RCS aggregator instead of entering into contract with every MNO to cover their target geographic region. Interestingly, MNOs can also play the role of RCS aggregator. Table 2 below compares the SMS and RCS channels.

	SMS	RCS
User experience	• Intuitive to use and there is no need for user training • Instantaneous access • Feature poor • Limited message size	• Can be intuitive to use, similar to SMS • Instantaneous access • Feature rich • Message size much larger than SMS (up to 20 kilobytes)
Availability	• Ubiquitous • Delivery cannot be guaranteed • Access over legacy technologies	• Becoming ubiquitous, needs support from MNOs, Platforms and OEMs • Provides delivery and read notifications • Access over various bearers

	SMS	RCS
Security	- Known vulnerabilities - Relies on implicit network authentication - Class 2 SMSs are encrypted	- Various authentication and security methods supported - No end-to-end encryption, however, hop-to-hop[6] encryption is used to support lawful interception - Verified Sender[7] [8]
Dependencies	- Works without data connection - App installation is not needed	- Needs data connection - Installing separate RCS client or use native messaging application with RCS support

Table 2 Comparing SMS and RCS Channels

3.2 RCS Security

3.2.1 Authentication mechanisms

Before a consumer can access any RCS service such as RBM several steps are needed to be completed as summarised in Table 3. Firstly, a valid configuration[9] needs to be set up in the RCS client and then authentication is required to access the service. Configuration is expected to be performed only when the phone is powered up with a new SIM inserted, or the first time RCS becomes available from the MNO.

Configuration	- When a device is ready for RCS configuration the consumer using that device is identified by using MSISDN or IMSI (if available) - Can be triggered by RCS client or the service - OTA provisioning of configuration data to the device - Trust in RCS client can be established by using tamper detection and integrity checking security mechanisms. For example, Google SafetyNet[10] on Android. - Device authentication is based on several methods and is dependent on the device profile and MNO ○ Header enrichment (mobile network-based identification/SSO) ○ GBA[11] (if supported) ○ OTP delivered to SIM over OTA-SMS - Digest authentication credentials (shared secret) for service authentication are provisioned to the device as part of the configuration. The secret information can be refreshed periodically by MNO

[6] Node to node
[7] Proof-of-Identity supported in RCS can be used by banks
[8] Note that in December 2019 Google launched Verified SMS on their own client in selected countries
[9] Service Provider Device Configuration, version 6.0, GSMA, 06 December 2018
[10] Google SafetyNet provides a set of services and APIs to detect device tampering, for example, if an Android device has been "rooted"
[11] see Appendix A.3 for details

Authentication	• Service level access to IMS (SIP) or data (HTTP) requires authentication by MNO • IMS access is SIM based on mobile network authentication (AKA[12]) • For data access there are several options[13] such as digest authentication that is provisioned at configuration, or SIM based methods such as the following o GBA o Open ID Connect[14] with Digest AKA or EAP-AKA

Table 3: Steps required before an RCS client can access any service

For the purposes of configuration, the consumer is identified by their MSISDN or IMSI where supported. RCS Service Provider (SP) uses an Over-The-Air (OTA) mechanism for provisioning device configuration. The configuration provisioning can be triggered either by the RCS client on the device or from the network side. The configuration data is downloaded to the device from the SP over a channel secured with Transport Layer Security (TLS).

The authentication mechanism to access the RCS service itself is mostly based on digest authentication (username and secret) that is configured by the MNO. The digest authentication secret can be periodically refreshed by the MNO and can be made complex without the consumer having to choose or remember any details. There are several options for authentication as proposed in the GSMA specifications[15] in order to securely access RCS services. Once the required steps are complete the RCS client is ready to receive any supported service such as RBM.

3.2.2 Sender verification

SMS has become a preferred channel for fraudsters for making unsolicited contact with consumers, for instance, sending malicious messages for phishing purposes. As highlighted in section 2.2.2 an underlying weakness with SMS is that it does not provide any assurance on the identity of the sender. A spammer can spoof the details of a legitimate sender and the consumer has no easy way of verifying the authenticity of the received message. RCS is capable of mitigating this with the Verified Sender security mechanism that is supported in RBM. Verified Sender provides a proof-of-identity of the message sender. The proof is based on a digital signature that is provided to the RBM platform and the MNO. For a consumer, this proof can appear as a tick-mark and a verified name and logo of the sender on the RBM client user interface.

With Verified Sender, service providers can get their RBM-based messaging chatbot verified by a Verification Authority (VA). VAs can be an independent entity, or existing players in the message delivery process, like an MNO or a third party. A brand sends a verification request [4, 5] to the VA who then formats the brand's information such as name, icon, and service identifier in a structured manner and digitally signs it. If verified, this information flows through the message delivery

[12] see Appendix A.3 for details
[13] see Appendix A.3 for details
[14] see Appendix A.3 for details
[15] In RCS Universal Profile Service Definition Document, version 2.2, 16 May 2018

process and is shown as a tick-mark on the messaging client installed on the consumer's device. Service providers may need to pay for the cost of the verification; this can be covered in the contract with MNO or a third-party VA. Service providers can choose to use Verified Sender to win trust with their consumers, and consumers on the other hand can be confident that they have been contacted by a legitimate party, for example, their bank.

3.2.3 Protection against 'SIM swap'

As noted in Section 2.2.2., a potential risk in using SMS for security purposes is exposure to fraudulent 'SIM swap'. Although RCS does not directly address this security threat, additional controls can be put in place by MNOs and service providers to protect their consumers.

The SIM identity, International Mobile Subscriber Identification (IMSI), is used by the MNO to identify and authenticate consumers to the network for providing access and for billing purposes. Whereas the mobile telephone number (MSISDN) is used by service providers such as banks to identify and authenticate consumers for account management, validating transactions based on OTP, etc. By design, both MSISDN and IMSI are not strongly linked with each other due to portability and MNO service configuration requirements. For example, an MNO consumer should be able to change his/her SIM and keep using the same mobile telephone number.

The fraudulent SIM swap scenario is based on fraudsters exploiting service providers' use of consumer's mobile number for identification and authentication purposes. Fraudsters using social engineering techniques can convince MNO staff to order a replacement SIM with consumer's (victim) mobile number, or they can impersonate a legitimate consumer to setup a new account and link victim's mobile number to fraudster's SIM identity. Having additional security measures can mitigate fraudulent SIM swap. These measures include requiring PIN or password to access consumer's account with MNO, or 2FA, and verifying this before any account management request such as SIM replacement is serviced.

With RCS, when a consumer orders a replacement SIM, if a configuration associated with the SIM is able to resolve the consumer's mobile number (MSISDN) or SIM identity (IMSI), then the service is readily reinstated [3, 6]. If not, all existing configuration and security association is invalidated, and service is newly provisioned starting with the discovery of a configuration server. In a scenario where the SIM is not in a ready state, i.e. either physically removed or powered off, RCS invalidates all existing security context.

Additional security controls are needed to mitigate fraudulent SIM swap to protect RCS consumers. In the event of a SIM swap, the MNO can take additional measures to verify the identity of the consumer. The MNO can also indicate SIM swap requests or transactions being made to the service provider such as a bank. The service provider can then take additional security measures and ask the consumer to verify his/her SIM swap, completing additional checks over a different channel, before OTP is sent over RBM.

3.3 Strong Customer Authentication based on RCS

3.3.1 Potential architecture for OTP over RCS

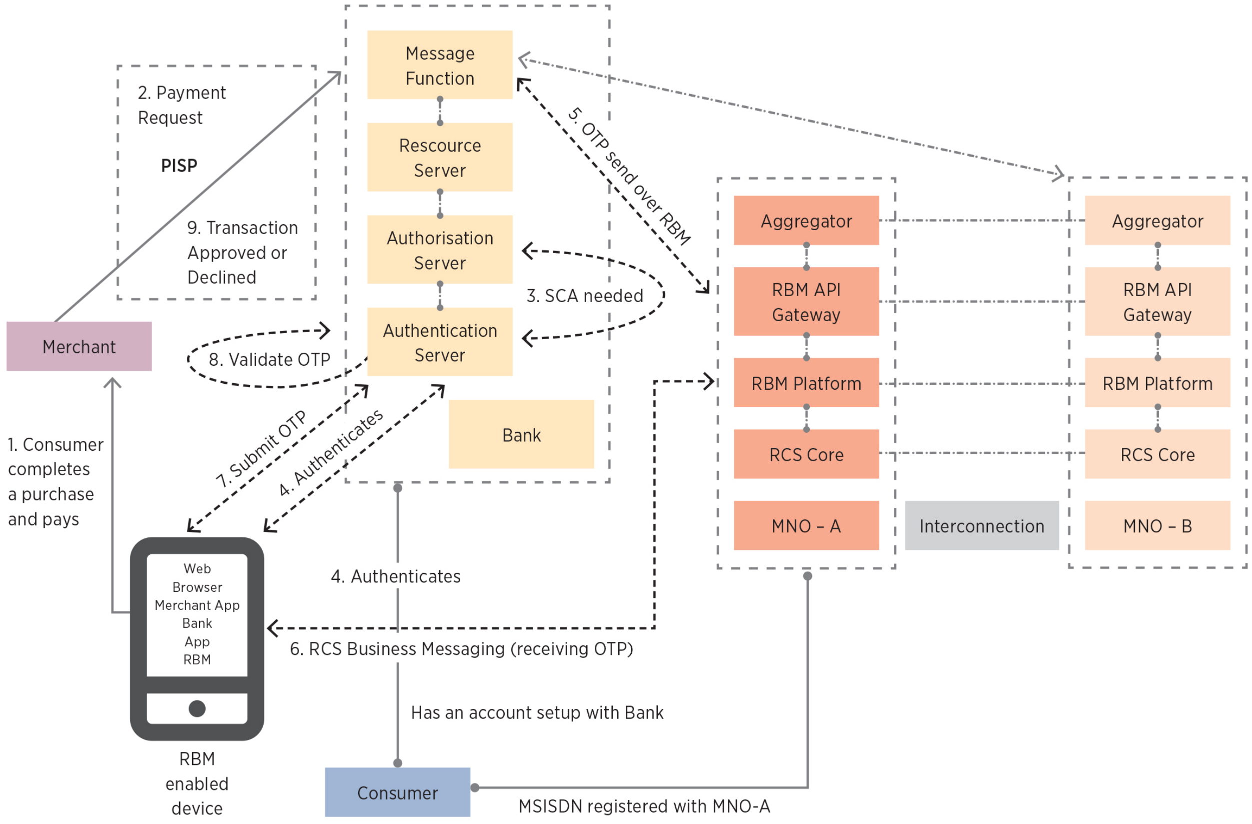

Figure 4: Potential Solution - OTP over RBM.

In this section, we discuss a potential solution where a bank uses OTP over RBM in order to fulfil SCA. This flow is based on Open Banking (OB) decoupled flow as described in [7]. We have removed some details so that the focus is on authentication. The diagram above shows a solution which can be summarised as follows:

1. The consumer has an account with their Bank and has a registered MSISDN with MNO-A (MSISDN registered to a SIM).

2. The consumer possesses a mobile device that functions with the registered SIM and the device is RBM enabled. We have not detailed the RCS configuration and authentication steps that are required to access RBM platform.

3. The consumer makes a purchase at a Merchant website on a web browser or on an app and chooses to pay with account (via the PSD2 payment API) and selects the bank from which payment is to be taken.

4. The Merchant collects the payment information and uses a PISP[16] to initiate PSD2 payment with the consumer selected bank. We have hidden the PISP and the full details of the Open Banking (OB) flow, a

[16] The actual process may involve intermediaries

decoupled flow in this case, for simplicity. Based on the transaction details bank decides to authenticate the consumer. Consumer is redirected to the chosen bank on a web browser or on a dedicated app or within RBM and starts the authentication process.

5. The bank receives confirmation from MNO-A that the consumer's device has been authenticated and is ready to receive RBM communication. The Bank chooses decoupled flow [7] and decides to send OTP to the consumer's device over RCS channel. The Bank uses RBM platform APIs to interact with and trigger messaging with the MNO-A.

6. When the consumer's device is connected, it receives the OTP over RBM. If the device is offline, the bank can choose to use the advanced message handling capabilities such as recalling an undelivered message.

7. With RBM, the consumer can utilise the Verified Sender feature to confirm the identity of the bank. Consumer can also then acknowledge receipt of the OTP to the bank by using RBM. The consumer then submits the OTP to the bank, on a web browser or on a dedicated app or within RBM, in order to complete the authentication process.

8. The Bank validates the OTP and computes an authentication code/result.

9. The Bank tells the Merchant (via PISP) the transaction result and the Merchant provides the result of the transaction to the consumer.

3.3.2 Advantages and challenges in using RCS

Here we briefly consider the advantages and challenges of using RCS for PSD2 SCA:

- How is device ubiquity addressed and will this effect deployment?

  GSMA Universal Profile was developed to harmonise RCS deployments globally. Barring Apple, the device OEMs and platform providers have offered wide support for native RCS clients. However, the service providers can address this limitation by leveraging downloadable clients. In Japan, the operators[17] have successfully launched a messaging service that conforms to GSMA RCS specifications and can reach consumers on iOS devices. In the future it is expected that the ubiquity of RCS will be similar to that of SMS.

- Is mobile data connectivity a limiting factor?

  Consumer may not be present in a geographical area with good coverage of mobile data services. This means unless there is Wi-Fi access RBM is not active and not ready to receive any communications. In such circumstances a bank can utilise advanced RBM capabilities. For instance, schedule a delayed delivery of bank's message with OTP until the consumer becomes active. Bank can also recall the message after expiry of specific period and force re-authentication.

- Is regional coverage a limiting factor?

  In terms of coverage although SMS offers great reach it has some limitations. Globally, RCS launches are growing in number, and with increased device penetration, service

[17] NTT Docomo, KDDI and SoftBank

providers can now plan to target a large addressable market.

- RCS implicitly guarantees possession

  SMS is accepted as proof of possession of the SIM hence an OTP delivered via SMS is supporting SCA possession. From a PSD2 context, RBM with OTP offers similar certainty as proof of possession of the SIM. However, in the future, interface with SIM or mobile OS platform (e.g. fingerprint biometric service) can possibly be defined for RCS client, and when that is implemented RCS can be used to support other SCA methods, for example, RCS client can possibly be considered as "software/app strongly linked to the device". With RCS-SIM interface defined, the SIM can generate a cryptographic code (e.g. one-time usable code/digital signature) that can be used by the Service Provider to authenticate the consumer. We note this approach may allow MNOs to play a key role in SCA. With interface between RCS and mobile OS platform defined, a Service Provider can potentially trigger the type of biometric verification (Inherence) to be completed (e.g. fingerprint/iris), or authentication via passcode (Knowledge), and get confirmation that the consumer has successfully authenticated or not from the OS service via RCS.

3.3.3 Using RCS for other SCA options

Our focus in this paper is exploring the potential use of RCS channel to deliver OTP over RBM. However, we think there are other methods and RCS features that may be considered to fulfil SCA requirements in PSD2. Banks can utilise RCS Chatbot features in RBM to service the SCA. We list a few other methods that can potentially utilise RCS channel and these need a further examination. Note, we are specifying these as potential future solutions for banks and MNOs to consider. There may be new specifications needed before they can be implemented.

- Using inherence elements in SCA
- Consumer may be prompted to complete a fingerprint based biometric authentication and the result of the authentication can be passed back to the bank over RCS channel. Other potential methods include voice recognition, retina/iris scan, facial recognition, measuring heart rate by interfacing suitable wearable accessories, registering and measuring keystroke dynamics and so on.
- Using knowledge elements in SCA
- Consumer may be prompted to complete a security challenge-response over RBM, and the result can be sent to the bank over RCS channel.
- Using possession elements in SCA
- Consumer may be asked to provide a digital signature or a code or a token that was computed by the device or SIM over RBM. This can be used as an evidence of possessing the device

4. Payments over RCS

This section looks at how payments can be configured to run using RCS with a focus on conversational commerce – the trend towards interacting with businesses through messaging and chat apps. Finding ways of monetising these conversations will only be effective if there is also a means of paying for them.

Details of how SCA works for each payment method can be found in Section 5.

4.1 Conversational Commerce and RCS

One obvious additional extension of current common payment solutions is via conversational commerce, where payments are embedded in online conversations such as those that occur via chatbots or through social media. Conversational payments are already widely used in China via WeChatPay and Alipay and attempts to replicate this in European countries are already underway.

Although there are many variations on the conversational commerce theme, they all involve serving consumers with opportunities to make purchases which, under SCA, will require consumer authentication. Nothing is more likely to disturb the flow of the conversation, and prevent purchases being made, than the intrusion of an awkward OTP based authentication process.

Using RCS and its rich messaging capabilities to run the conversational commerce programs and embedding SCA within this via behavioural biometrics and unique identification of the messaging app would provide a simple curated payment experience with minimal intrusion as long as consumers had previously set up a payment method.

4.2 Moving from Conversation to Payment

Under RCS, in the context of conversational commerce, there are a range of possible methods for payment integration:

- Use of a dedicated authentication / payment chatbot
- Using a 3rd - party or MNO application
- Accessing a payment method via a web browser
- Accessing a payment method via a web view
- Using x-Pay payment capabilities

4.2.1 Dedicated Authentication / Payment Chatbot

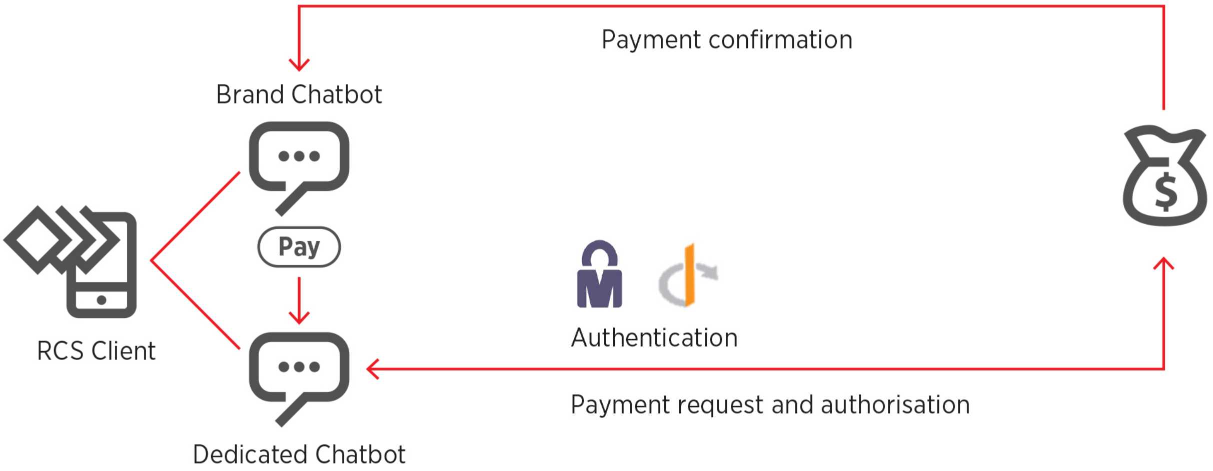

Figure 5: Dedicated Chatbot

Here the RCS client is integrated to the primary chatbot of the organisation mediating the conversations – which could be a social media network, an MNO, a retail organisation or any entity that needs the ability to take payments in the context of online conversations. When the consumer hits a **Pay** button (sent in chatbot thread e.g. as a RCS chip) this redirects to a secondary dedicated chatbot that is responsible for managing the authentication and payment process. At this point the consumer is now interacting with the dedicated authentication / payment chatbot.

Typically, the authentication and payments messages are now being sent either to a Payment Gateway, which will identify the payment methods available (e.g. card, PayPal, etc) and which will help to manage the authentication process, or to the MNO as a DCB payment request. Once the consumer has authenticated and the payment provider has authorised the payment the payment confirmation is then returned to the original chatbot.

Pros and Cons

As solutions go, this has the advantage that there is no client integration, and the consumer is retained within the client. The MNO has control over how the consumer's personal data is shared, and the authentication/payment chatbot will provide consistent behaviour.

On the downside, the effect of passing over control to a secondary chatbot may impact the look and feel of the whole experience – and any problems with the authentication and payment chatbot may lead to consumer dissatisfaction with the provider of the primary service. The redirect process between primary and secondary chatbots may also lead to issues in the threads of conversation – using an RCS A2P message is one option; however, RCS P2A deeplinks (if supported by client) would deliver a superior chatbot thread switching UX.

Security Considerations

- RCS clients should verify the authenticity of the chatbots to which they connect. This can be achieved using the Verified Sender service.
- The service provider should ensure that chatbots receiving any payment information are connected to a legitimate RCS client.

- The device OEM should ensure any RCS client is not modified since it was released, e.g. using integrity checks. The service provider and MNO could potentially rely on such assurance from the OEM. For example, the RCS client should not be running on a device that has ‘root access’ or is ‘jailbroken’.

4.2.2 Payment Application

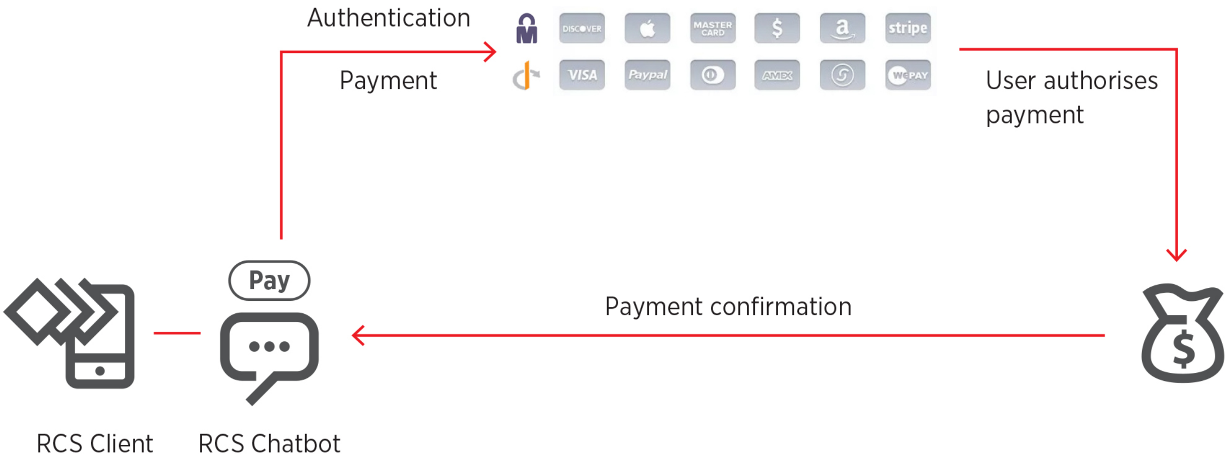

Figure 6: Payment Application

Under this scenario, a chatbot message is used to offer the consumer the opportunity to hit a Pay button (sent in chatbot thread, e.g. as a RCS chip) and the RCS client will then connect to a 3rd-party (e.g. PayPal) or MNO app (which has registered a URI handler with the OS) to manage the authentication process. Once authenticated then the associated payment app is opened via a deep link, available payment methods are presented – e.g. PayPal or DCB – and the payment is authorised. The payment confirmation is then returned to the consumer via the chatbot thread, and the consumer can pick up the conversation where they left it.

Typically this requires authentication to be done by the MNO or third-party – which is allowed under PSD2 only if the payment instrument issuer has an agreement with the authenticating entities. PayPal, for instance, will already be an authorised payment service provider, but each potential payment instrument provider needs to be assessed on its own merits. Again, note that the rich messaging capability of RCS allows for a more complex and potentially frictionless authentication experience.

Pros and Cons

The use of existing apps from third-parties or MNOs reduces integration effort – the payment process can interoperate with either DCB or a third-party payment processor, using existing solutions. It will generally be a familiar process for the consumer.

On the downside the consumer is directed out of the conversation in order to authenticate and pay and may need to download a separate application to enable this. For the brand managing the conversation this can lead to complicated integration processes – and may impact the brand itself if there are problems in the authentication or payment processes as consumers will tend to assume that the entire process is brand managed.

Security Considerations

- The handover to 3rd party or dedicated payment apps via deep-linking needs to be carried out securely in such a way as to protect the confidentiality of any sensitive data such as consumer payment information

4.2.3 Web Browser

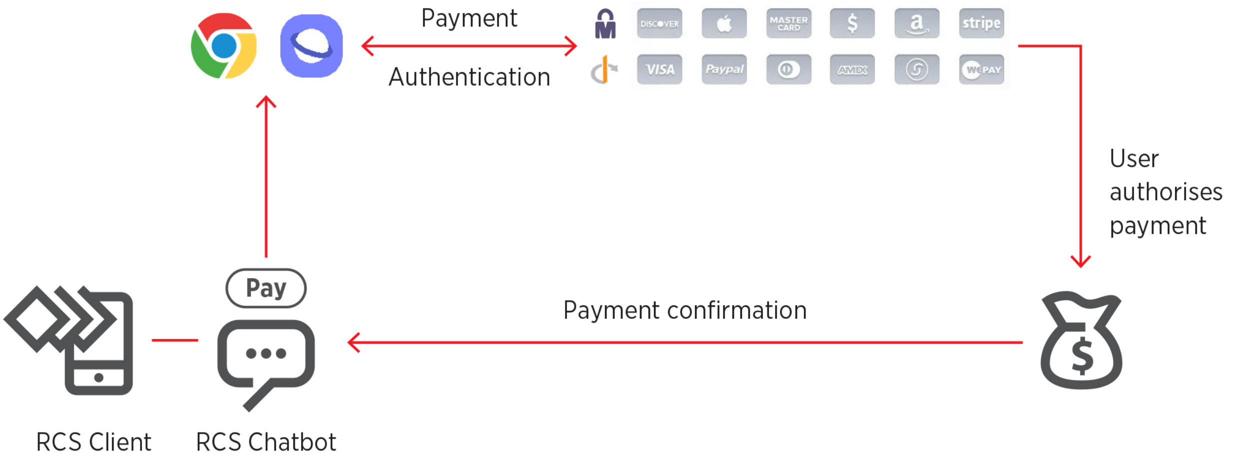

Figure 7: Web browser

In this scenario the consumer is selecting a **Pay** button sent in chatbot thread which then triggers a browser to manage the authentication. The advantage of this is likely to be that a browser-based authentication flow will be a familiar consumer experience. Once redirected to the website the authentication and payment process will be determined by the website implementation which, in theory, could access any available payment instrument.

In an ideal process the browser will present the consumer with the available payment methods, the consumer selects the method and authentication and authorisation of the payment are completed on the web. The RCS client can serve the browser with device information as part of the authentication process, which under some scenarios – particularly card based or direct to bank API payments – can reduce the over rates of SCA applied as the bank can perform risk-based authentication.

Once authorised the payment is confirmed back to the RCS chatbot which returns the consumer to their conversation.

Pros and Cons

This may be a very familiar experience for the consumer, and it allows the use of the full range of existing authentication and payment options – however, because it will involve additional apps or any client integration it needs to be carefully designed to ensure it is a seamless experience for the customer.

However, the process may be controlled by the brand or a payment service provider, whose website mediates the process, meaning that the MNO could lose control of the process as the consumer leaves the RCS chatbot in order to make the payment.

Security Considerations

- A potential security risk is re-directing the consumer to a malicious website for phishing purposes. As a countermeasure the MNO or RBM provider can use a whitelisting security mechanism or look-up a blacklist to ensure that the consumer is redirected to a legitimate party, i.e. a bank's server/endpoint
- Another potential risk is malicious browser plugins or extensions could be used to capture sensitive information such as payment details. As a countermeasure the device OEM should ensure the integrity of the web browsers allowed

4.2.4 WebView

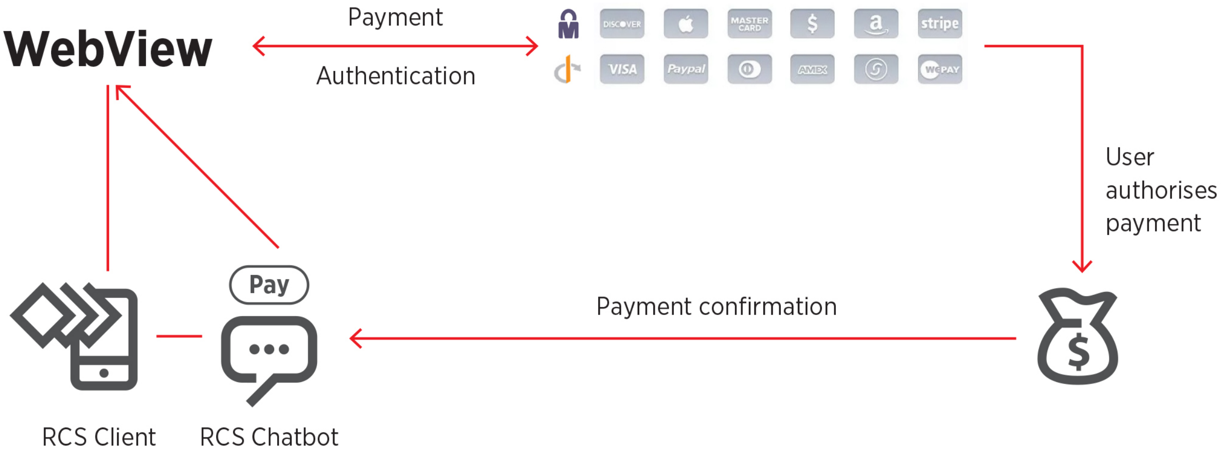

Figure 8: Webview

WebViews are browsers bundled within mobile apps – essentially, they allow the display of webpages inside the app. Using a WebView will be a similar experience to using a browser for the consumer.

The RCS chatbot allows the consumer to hit **Pay** and the redirects to a WebView for authentication. This opens the available payment methods allowing the consumer to select their preferred payment instrument and to authenticate and authorise the payment. The payment is confirmed to the chatbot and the consumer is returned to their conversation.

Pros and Cons

The consumer is offered a familiar experience with access to a full range of standard authentication and payment options via MNO DCB or a third-party payment process. The consumer also stays within the client, meaning there should be a seamless transition between the stages of the transaction.

On the negative side, this is a client feature which needs to be agreed between clients in order to ensure a universal customer experience. In addition, because the process is controlled by the brand the MNO may lose control of the payment process, reducing their commercial opportunities.

Security Considerations

- WebViews need to be configured so as to mitigate any potential security risks. The risks include, data exfiltration due to malicious JavaScript being executed, loading web resources in an insecure manner, deep-linking issues, and having access to device resources such as files
- Similar to web browsers, the MNO or RBM provider could use whitelisting to ensure only known legitimate web resources are allowed to be accessed over WebViews

4.2.5 X-Pay Integration

'X-Pay' or OEM Pay solutions such as Google Pay or Samsung Pay are grandfathered into SCA compliance and offer a familiar experience for consumers that have enabled these features. The current X-pay solutions use tokenised payment cards – essentially the real card number is replaced by a transactable "token" which can only be used from the x-Pay application, although this may change in future.

Both Google and Samsung have integrated their X-Pay solutions into their respective browsers– allowing these methods to be used to make payments when a browser payment is triggered – and therefore can be considered as specific payment instrument type in the browser or WebView payment scenarios.

Alternatively, both Samsung and Google may provide APIs that would allow an RCS client to trigger authentication and payments directly, with the consumer being directed to the x-Pay apps in order to authenticate and authorise the payment before being returned to their conversation.

Pros and Cons

The familiarity of this process is a big advantage for consumers – and the ability to integrate these methods into an RCS mediated transaction process with full SCA compliance is a big advantage. There is no investment required by MNOs and the security processes around tokenization means that the security risks are minimal.

However, it should be noted that x-Pay implementations have not been universally adopted and that they would require client integration to make them work. In addition, without the OEM in question agreeing there are issues in integrating proprietary payment methods such as DCB. In general, the OEMs will levy significant fees on brands using their payment methods to purchase digital goods or services – up to 30% in some cases – so the business case for brands will need careful consideration. Also, the MNO will lose control of the payment process, while the OEM may gain access to personal data of the consumer.

4.3 Payment Manager

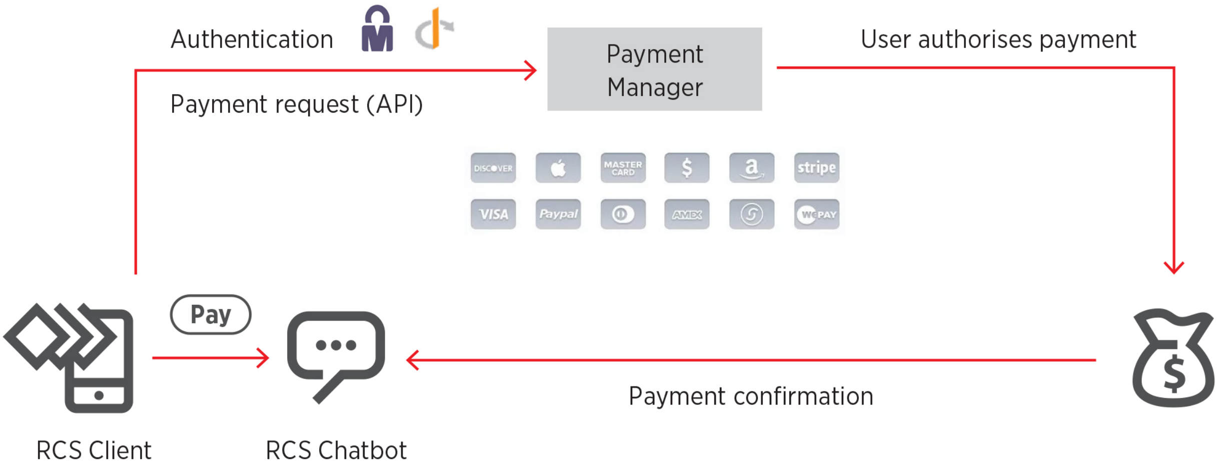

Figure 9

Many of the Many of the actual methods above may integrate to a Payment Manager selected by the MNO – also often referred to as a Payment Processor or Payment Gateway. These organisations provide a single API towards brands to allow them access to multiple payment options and also to shield them from changes to the underlying payment solutions that they give access to – hence for many brands using a Payment Manager will increase their acceptance and conversion rates.

In this scenario when the consumer hits **Pay** in the RCS chatbot thread the client will direct them, via WebViews or a 3rd-party application to the Payment Manager. Note that authentication can be applied separately or may be performed by the Payment Manager as part of the payment process.

The consumer will select the payment method they prefer and the payment confirmation will be sent by the Payment Manager back to the chatbot to allow the consumer to resume their conversation.

The Payment Manager provides MNOs and brands with a wider range of payment options and can enable proprietary / alternative payment methods such as DCB, Mobile Money or local stored value solutions. MNOs managing this process can curate the payment methods offered – adding or removing them as they wish.

This allows the MNO to retain some control over the payments process and has the advantage of being accessible through a range of different methods. Note that in some cases liability may pass to the MNO, although under PSD2 this is only the case if the MNO is acting either as or on behalf of a regulated payment service provider.

5. Using RCS to Enhance Existing Payment Methods

5.1 RCS and SCA

Although the focus of this paper is largely on comparing the relative merits of SMS and RCS as methods of carrying OTPs, perhaps the more important point is that while SMS can support a single factor – possession – using a single method – OTP – RCS can support a broad range of alternative factors. It's true that RCS is, in most circumstances, a better option for carrying an OTP – particularly if Verified Sender is being used, which means that where available it can be used as a like-for-like replacement of OTP-over-SMS. However, it's when looking at a broader range of scenarios that the true advantages of a pervasive RCS solution become apparent.

PSD2 enforces SCA on all electronic payments initiated by the payer bar where exemptions apply. A full treatment of exemptions shows that their application is complex and will lead to varying outcomes – a far better solution would be to find methods of performing frictionless SCA to ensure consistency of outcomes.

Potentially there is a vast range of payment scenarios where SCA will be required and in this section, we examine a few of the more common ones to show where RCS can be used to improve the consumer experience.

5.1.1 SCA on Mobile Devices

In the context of the user interaction options outlined above we can briefly examine how SCA can be performed in each of these. Noting that SCA requires two independent factors out of possession, knowledge and inherence, the main options are:

- **3rd-party app** – most likely a banking app, which manages the two-factor authentication process. Note that this may be separated into a banking app and a separate authentication app. As the app will be controlled by the consumer's bank, the liability for authentication rests with the bank. Critically the app must be cryptographically pinned to the mobile device to prevent it being cloned – without this the possession factor is lost

- **Mobile Connect two-factor** – usually supported via an SDK, this allows the authentication process to be controlled by the MNO. Providing the authentication factors meet the requirements of SCA then this offers a standalone authentication option. However, under PSD2 for this to be accepted either the MNO must be a regulated payment service provider – essentially a bank – or must have bilateral agreements in place with the banks it supports SCA for

- **Redirect mode** – this is typically either an app-based or browser-based process, potentially mediated by the Payment Manager as part of the payment flow. The authentication process is redirected to the consumer's bank who determines the authentication steps to be followed

- **Decoupled mode** – this is where authentication takes place entirely on the mobile device; a commonly used approach for x-Pay solutions. To be permitted under PSD2 the x-Pay providers must have bilateral agreements in place with all of the consumer banks that they are supporting

In the context of RCS and SCA we would also note that behavioural biometrics are a permitted inherence factor – see Section 5.3 for more details.

5.2 Payment Methods

Broadly there are seven methods by which a consumer can make a mobile payment:

- Card payments, specifically card-not-present or ecommerce transactions
- Direct from account or push payments such as offered via the PSD2 Payment Initiation API
- X-Pay solutions such as Apple Pay or Google Pay, using a payment card tokenised or aliased onto an app
- Payment Aggregation Gateways such as PayPal who can direct payments to a range of different providers via a standardised API
- Direct Carrier Billing (DCB) where the payment is made directly against the consumer’s mobile phone bill
- 3rd Party Wallets where payment instruments – usually but not solely payment cards – are stored, usually in the cloud
- Mobile money solutions where the provider has a store of value available to transact against

Under PSD2 all of these payment methods constitute electronic payments and are all fully subject to SCA apart from DCB. PSD2 specifically limits the use of DCB to digital products and services to a value of €50 per transaction and €300 cumulative total per month – however, within these limits DCB is exempt from SCA. However, these rules only apply within the European Economic Area.

5.2.1 Card Not Present / Ecommerce payments

Card payments are the single most common form of payment method for payer-initiated transactions over the Internet. Considerable effort has been expended by the EBA to design SCA and exemptions to provide backwards compatible support for card payments since, clearly, any impact on these would have a damaging impact on ecommerce transaction volumes. Most of the SCA exemptions were designed with card payments in mind.

Unfortunately, Card Not Present (CNP) transactions lend themselves very poorly to SCA. The standard industry response to this is to use 3D-secure, which allows merchants to forward transactions to an issuer for pre-authorisation before launching the payment transactions. Rates of transaction abandonment on 3DS were so high many merchants preferred to ignore it and take on the fraud risk themselves. PSD2 blocks this option so EMV Co have developed a new version of 3DS to try and remove many of the issues.

Under 3DS issuers will decide whether SCA is exempted or is required. If required then the issuer has two options – to either send a direct authentication request back via the 3DS channel or to deliver an out-of-band (OOB) authentication request. In both cases one of the possible authentication factors is an OTP-over-SMS. The use of RCS to replace this could lead to a much-improved experience for cardholders:

In the case of an OOB authentication request we would expect to see an authentication request pop up in an authentication app – probably, but not necessarily, a banking app using an MNO client or an MNO authenticator app. The cardholder can then either authenticate directly to the app, which should generate an encrypted token in response which the operators can check, or can use a smartphone's own authentication capability (e.g. biometric). The app, pinned to the phone, represents the possession factor and the authentication the second factor either using biometrics for inherence or a knowledge-based item such as a passcode.

Using RCS allows MNOs to provide an encrypted and protected channel which they can either use to create an authenticator app or they can parlay into an authenticator capability which the banking app itself can use. We regard as important that an authenticator capability could potentially be used for other types of payment channel.

In the case of an in-band authentication via 3DS-2 then the current implementation only supports possession and knowledge factors. In this case an OTP over RCS provides a more secure version of OTP-over-SMS but can only be used in the same way – either as a possession factor that can be entered into a browser payment on a secondary device (e.g. laptop) or used in the payment app on the same phone – which is permitted under PSD2 as long as the authenticator app / channel is demonstrably independent of the payment app channel. RCS clearly meets these conditions. This is not an ideal scenario, but this is a limitation of the existing channels.

The rich messaging features supported by RCS can bolster this process in both directions. Messages received by the consumer can be enhanced with personalised information and supported by Verified Sender to provide a baseline for assurance that the consumer is not being phished. In response authenticator apps can return a wide range of device information to allow the MNO or issuer to verify the device / consumer combination. As discussed below this opens up some very interesting options around behavioural biometrics.

In short: fully enabled RCS would provide significant benefits to issuers and consumers as a method of supporting SCA for card payments.

5.2.2 PSD2 / Account based push payments

PSD2 API payments are a form of push payments where the payer pushes funds from their account to a merchant or other payee. Although the PSD2 APIs will be pervasive there is a range of existing push payment solutions already being widely used in Europe such as iDEAL (Netherlands), Sofort (Germany) and MobilePay (Denmark). SCA solutions for these types of payment are roughly divided into two:

1. methods that redirect to the issuers – a similar process to the 3DS methods described in the card payment section; and
2. methods that rely on on-device biometrics.

Given the pervasiveness of the PSD2 push payment APIs – every account in the EEA will be enabled – and their inherent suitability for mobile payments we expect a reasonable and growing adoption of these. This will likely be driven by retailers looking to reduce the costs and improve the security of their online payments process rather than as a wholesale replacement for online card payments.

In redirect models then the consumer is directed to their bank where they will be required to authenticate themselves under SCA. Typically, this would be an OOB process similar to that described for card payments under 3DS. There is no standard for this – issuing banks are at liberty to design their own processes. However, using RCS they can either push OTPs for use in secondary devices or apps or simply use the capabilities of RCS in-app to manage an enriched authentication process using knowledge or biometric elements. As long as the app is pinned to the device – i.e. it can only be installed on the specific consumer device – then this fulfils the two independent criteria for SCA.

A combination of push payments and rich messaging services in-app potentially offers an exciting solution for third-parties such as retailers wanting to offer their customers a low cost, high security payment service in the context of an on-line shopping experience. We would also expect issuing banks to be eager to take advantage of the enhanced security properties of RCS over SMS in order to help them comply with the fraud and risk requirements of PSD2.

5.2.3 X-Pay and Wallet payments

The other common form of online payments are via the 'x-Pays' such as Apple Pay and Google Pay or via payment wallets such as offered by third-parties like Visa and Mastercard. Although superficially similar these are different products under the surface and need to be considered separately.

X-Pay implementations are controlled by the mobile handset provider and use native OS capabilities to provide services, including authentication. The payment instrument currently is a payment card stored in the device's payment app. Typically authentication is achieved through a combination of handset biometric or passcode and the ability of the provider to uniquely identify the device. Some combination of the device and cloud-based servers generate cryptographic tokens as a result of the authentication which can then be verified by the underlying card issuer.

We would note that technically a similar setup would work if x-Pay implementations used non-card payment products: connecting push payments for instance. As this payment ecosystem is entirely controlled by the x-Pay providers the use of RCS or other technologies is entirely within their gift.

Wallets, although superficially similar to x-Pay solutions, are apps loaded on mobile devices and populated with payment instruments by trusted third-parties. Typically, the wallet app itself and/or the payment instrument issuer determines the authentication process to be used which would usually be some combination of methods previously discussed – including OTP-over-SMS. We believe that wallet providers may well be interested is using RCS as an authentication channel, both in order to carry authentication and device data but also as a means of carrying richer data to improve the consumer experience.

5.2.4 MNO Direct Carrier Billing

PSD2 restricts the use of Direct Carrier Billing (DCB), where payments are billed directly to a consumer's MNO account, to the provision of digital or voice services for less than €50 per transaction and a cumulative amount of €300 per month. Outside of these limits SCA applies.

Currently this makes the provision of DCB-like services difficult – applying SCA for purchases of physical goods or for higher value items is a poor consumer experience especially given the relatively low friction that they would have previously experience on this channel. However, if the purchases were made via RCS then applying SCA through any of the methods previously discussed becomes much more effective – and this immediately re-opens the door to DCB solutions.

Unfortunately, the catch in this is that only regulated payment service providers can implement SCA – although they can delegate SCA to a third party such as Apple or Google. So for an MNO to implement a DCB-like service over RCS they would need to either obtain a payment license – most probably an electronic money license – or partner with a regulated payment service provider. By definition this would also mean separate statements for the DCB-like purchases, although nothing prevents these from being added to and itemised in a consumer's mobile phone bill.

In short RCS would allow a more customised, secure experience for DCB-like payments under PSD2 but would come at the cost of additional regulation for either the MNO or the service provider.

5.2.5 Mobile Money

Direct integration of a mobile money account into RCS would offer significant user experience advantages, with a highly accessible and easy-to-use front end interface. RCS messaging clients currently haven't enabled P2P payments among users so the triggering for such a payment would have to be an additional feature. However, mobile money providers and the enterprises/merchants using it could benefit from increased B2C capabilities, as seen in existing use cases and successful campaigns.

An easy first step for the integration of mobile money into RCS could be through a dedicated chatbot (as described in the section above), which would act as the user's mobile money account, adding smart functionalities and an intuitive interface, without the need for a large investment that a smartphone app would require. It's also good to note that some device manufacturers have already started installing RCS enabled clients on smart feature phones.

5.2.6 Aggregators

Aggregators (e.g. PayPal) provide access to payment instruments. The banks or payment account providers are responsible for SCA and will determine the form of SCA required – see other subsections for examples.

5.3 Behavioural Biometrics

Most current inherence factor implementations are relying on on-device biometrics such as fingerprint or facial recognition where the device can assert consumer authentication to an issuer through a verifiable cryptographic token. This, coupled with app pinning for possession, provides a relatively frictionless way of fulfilling the SCA requirements.

However, the PSD2 requirements leave the door open for providers to develop behavioural biometrics to fulfil the inherence factor. Risk based analysis using data such as keypad pressure, device location and device fingerprinting is already used by many issuers and risk management companies to assess the probability that the genuine consumer is making requests. Extending these capabilities to a full behavioural biometric which is used to authenticate the consumer without their direct intervention is entirely achievable.

However, at the moment the secure channels to deliver this are dependent on individual implementations. Using RCS to provide an implementation independent channel for delivering the relevant data to allow a completely frictionless authentication process seems like an obvious step forward subject to regulators being convinced of the accuracy of the process.

6. Benefits to consumers, card issuers, and banks

Placed in the context of PSD2 and SCA, RCS offers huge potential for improving the payment experience across a whole range of use cases. In particular there are two aspects of RCS that apply across the different payment scenarios – improved security and a better customer experience.

Banks and regulators remain concerned about the various flaws in SMS security – particularly SIM swap attacks – but have reluctantly concluded that the flaws in OTP-over-SMS are outweighed by the overall improvements. In essence SIM swap attacks are socially engineered one device at a time – which is painful for the individuals – but this is a vast improvement on wide-scale attacks using, for instance, databases of stolen cards with no inherent authentication at all.

In this environment we expect that criminals, blocked from easier attack vectors, will switch their attention to other known weaknesses – for instance, targeting SIM swap or phishing exploits. As such the ability of RCS to provide Sender Verification and to offer improved levels of security over SMS immediately makes it of value for banks and regulators.

In respect of customer experience, RCS allows banks to extend their payment offerings to customers who do not necessarily use their banking app and still offer them an enriched experience – for instance to provide up-to-date information about previous transactions or current balance, and the status of the current payment.

Critically, though, it will allow the creation of better and rather frictionless authentication journeys across a range of different payment use cases in the area of conversational commerce. Applied effectively RCS based authentication journeys have the opportunity to displace all other authentication methods, apart, perhaps, from those of the x-Pays, whose dominant position in some markets allows them to decide for themselves how they wish to proceed.

The other side of this is the consumer experience – and this will be significantly improved by the advent of RCS. The existing OTP-over-SMS processes offer a very poor experience and are only tolerated on the basis that there is nothing better to use. Even replacing OTP-over-SMS with OTP-over-RCS would be a significant improvement in terms of ensuring that customers are not being phished.

However, when we add to this the potential enhanced possibilities for other forms of frictionless authentication factors such as behavioural biometrics or transmission of real-time biometric information in conjunction with Verified Sender and enriched customer data it is clear that RCS will be a vast improvement on anything widely available in the market today.

As banks have realised, under PSD2 mobile devices are the preferred method of performing SCA. RCS will improve the customer experience, reduce the fraud risks and improve adoption of mobile based authentication methods. This is a win-win for banks and consumers.

7. Conclusion

The use of RCS and RBM offer significant advantages to all parties involved in mobile based authentication and payments. In the context of OTP-over-SMS the use of RCS is potentially a major improvement in terms of security and information exchange, helping to reassure consumers that they are in communication with a genuine authentication provider while providing the authentication and payment service providers with a rich stream of data to use to manage risk and fraud.

As it stands SMS is still better than existing on-line authentication tools, but this paper's overall observations are:

- SMS offers great reach but has limitations
- The combination of RCS launches and device penetration means an increasingly larger addressable market, moving towards ubiquity similar to that of SMS (depending on Apple launch in certain markets)
- RCS can replace other channels - app usage has stagnated such that 22% are only used once 25% are deleted after one use. RCS and RBM provide brands with a powerful and potentially more secure way of reaching, engaging and monetising consumers

The natural integration of RCS into conversational commerce could be limited by difficulties in enabling authentication and payments. However, as we have shown, this need not be the case subject to the appropriate integrations being performed. Not only does RCS allow integration with most existing payment solutions and platforms it also offers significant advantages in terms of consumer authentication, particularly in the context of SCA.

In the SCA context banks have a critical requirement to be able to authenticate consumers without introducing friction into the process. The ability of RCS/RBM to provide risk management data to allow both device and consumer identification without direct intrusion into the payment process will likely drive banks to adopt RCS as soon as it is practically feasible.

References

[1] RCS Universal Profile Service Definition Document, version 2.2, GSMA, 16 May 2018.

[2] Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2), EBA/RTS/2017/02, 23 February 2017.

[3] Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2, EBA-Op-2019-06, 21 June 2019.

[4] Rich Communication Suite 9.0 Advanced Communications Services and Client Specification, version 10.0, GSMA, 06 December 2018.

[5] RCS Verified Sender Product Feature Implementation Guideline, GSMA, March 2019.

[6] Service Provider Device Configuration, version 6.0, GSMA, 06 December 2018.

[7] Open Banking Customer Experience Guidelines, Open Banking Limited, Version 1.2, 14 March 2019.

Acronyms and abbreviations

The following acronyms and abbreviations have been used in this document:

Term	Definition
API	Application Programming Interface
ASPSP	Account Servicing Payment Service Provider
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ID	Identity
IP	Internet Protocol
MFA	Multifactor Authentication
OB	Open Banking
PISP	Payment Initiation Service Provider
PKI	Public Key Infrastructure
PSD2	Second Payment Services Directive
PSU	Payment Services User
REST	Representational State Transfer
RTS	Regulatory Technical Standards
SCA	Strong Customer Authentication
SMS	Short Message Service
TLS	Transport Layer Security
TPP	Third Party Provider
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

This Appendix contains information used in the analysis to produce the material in the main body of this White Paper.

Appendices

This Appendix contains information used in the analysis to produce the material in the main body of this White Paper.

A. Relevant requirements for SCA in PSD2

Relevant requirements for SCA in PSD2	
Article 4: Authentication Code	• Authentication to be based on two or more elements[18] categorised as knowledge, possession and inherence, and to result in the generation of an authentication code • Authentication code shall be accepted by payment service provider only once • Authentication code shall not reveal any elements of SCA • It is not possible to derive new authentication code based on knowledge of any other previously generated code • Authentication code cannot be forged • Any failed authentication attempts must be limited (up to five attempts) within a given period of time and must lead to temporary or permanent block • Communication sessions are to be protected against capture of authentication data and integrity protected from unauthorised parties • The maximum timeout after being authenticated and without activity shall not exceed five minutes which means consumer may need to be re-authenticated if needed.
Article 5: Dynamic Linking	• Authentication code generated shall be specific to the original amount of payment transaction. Any change to amount will result in invalidation of authentication code • Payment service providers shall adopt security measures to ensure confidentiality, authenticity and integrity of amount of transaction and information displayed to consumer.

[18] In order words, the elements of SCA

Relevant requirements for SCA in PSD2	
Article 6: Requirements of the elements categorised as **Knowledge**	• Knowledge element is something that only consumer knows • Payment service providers shall adopt countermeasures to the risk that elements of knowledge are uncovered or disclosed to unauthorised parties. The use of knowledge factor is also subject to the same mitigation steps • EBA opinion[19] is that knowledge element can constitute • Password • PIN • Knowledge based challenge-response • Passphrase • Memorised swiping path (not keystroke dynamics) • Knowledge element should exist prior to initiation of payment or account access

[19] https://eba.europa.eu/documents/10180/2622242/EBA+Opinion+on+SCA+elements+under+PSD2+.pdf

Relevant requirements for SCA in PSD2	
Article 7: Requirements of the elements categorised as **Possession**	• Possession element is something only the consumer possesses • Payment service providers shall adopt countermeasures to the risk that elements of possession are not used by any unauthorised parties. The use of possession factor is also subject to countermeasures that can prevent any replication • Having adequate security features such as algorithm specifications, key length and information entropy • EBA opinion is that possession element can constitute • A device where there is reliable means to confirm possession through generation or receipt of a dynamic validation element on the device • One-Time-Password (OTP) generated by software or hardware, as a token or as a text message (SMS) or as a push notification. In case of SMS, the possession element is the SIM card that is associated with the MSISDN that received the SMS • Printed OTP lists does not constitute as a possession element • Mobile apps, Browser or exchange of cryptographic keys provided that there is device binding to ensure a unique connection between consumer's app or browser or cryptographic key and the device used for payment initiation or account access. The binding can be achieved by hardware based secure element in a device or using a private key to link app to a device or registering browser to a device • An app or a browser that does not ensure a unique connection with a device does not constitute a possession element • Digital signature • QR code where device is evidenced by scanning with an external device • Dynamic card security codes (dynamic CVV) • Printed CVV does not constitute as a possession element

Relevant requirements for SCA in PSD2	
Article 8: Requirements of devices and software linked to elements categorised as **Inherence**	• Inherence element is something the consumer is • Payment service providers shall adopt countermeasures to the risk that elements of inherence are uncovered by any unauthorised parties. The access devices and software shall ensure a low false acceptance rate. The use of inherence factor is also subject to countermeasures that can prevent any unauthorised use through access to devices and software • EBA opinion is that inherence element can constitute • Biological and behaviour biometrics • Fingerprint, retina, iris scanning • Voice recognition • Vein recognition, hand face geometry • Keystroke dynamics • Heart rate or other body movement patterns that identifies consumer • Angle of device being held • Is dependent on the quality of implementation • Information transmitted using communication protocol such as EMV 3D Secure does not constitute as an inherence element as none of the data points or their combination exchanged through this communication tool appears to include any biological and behavioural biometrics • Memorised swiping path does not constitute as an inherence element
Article 9: Independence of the elements	• Payment service providers shall ensure that breach of any one of the elements does not compromise reliability of the other elements • Payment service providers shall adopt security measures to ensure protection to SCA elements or authentication code used in a multi-purpose device from being compromised. Such measures are as follows: • Separated secure execution environments through software installed in multi-purpose device • Mechanisms to prevent tampering software or device

B. Relevant requirements on communication channel in PSD2

Relevant requirements on communication channel in PSD2	
Article 25: Requirements for identification	• Payment service providers need to ensure secure identification of payer’s device and payee’s acceptance device for electronic payments including but not limited to payment terminals • Payment service providers to mitigate any risks arising from misdirection of communication to unauthorised parties
Article 26: Traceability	• Payment service providers to ensure all payment transactions and other interactions with consumer including merchants are traceable • Payment service providers to ensure • Unique identifier for the session • Logging of transaction details including transaction number, timestamps, and all relevant transaction data • Timestamps based on unified time-reference and synchronised to an official time signal
Article 30: Security of communication session	• ASPSPs and TPPs to ensure that data exchange via Internet is secured and to safeguard confidentiality, integrity using strong and widely recognised encryption techniques • ASPSPs and TPPs to ensure security credentials and authentication codes are protected from staff reading it at any time and any loss of confidentiality to be informed to the PSU without any undue delay and the issuer of the security credentials

C. Security mechanisms for RCS clients

Security mechanisms for RCS clients		
User Authentication Methods	**SIM based Authentication and Key Agreement (AKA):** This method relies on implicit authentication that is based on secret key stored in the SIM and the network authentication centre. AKA support entity authentication, message integrity, and message confidentiality. This implicit authentication can be extended by utilising Generic Bootstrapping Architecture (GBA/GAA) as defined in 3GPP TS 33.220 to derive new key material from AKA in order to establish new security associations as needed between the RCS client and the target RCS service.	Comments: To mitigate SIM-Swap fraud any security association established with implicit authentication and GBA/GAA must be invalidated upon a change of a SIM.
	Basic or Digest Access Authentication: User name and password (access credentials) is exchanged between RCS application and RCS service. A separate step called device provisioning is used to establish the access credentials. These user credentials are stored on the device and utilises platform provided stores mechanism such as Android KeyStore.	Comments: This method on its own is vulnerable to SIM-Swap fraud. However, security measures such as tamper-proofing and integrity protecting credential store on the mobile device; and verifying the RCS client's authenticity can be used to avoid any potential spoofing attacks.
	Network Single Sign-On: This method is based on utilising implicit network authentication and using IP address assigned to the device in order to identify the RCS client	Comments: This method is potentially vulnerable to IP-spoofing attack.
	One-Time-Password (OTP): In this method, an RCS client is validated based on an OTP (token) received on another device via SMS, or an external token service. Based on successful authentication a long-term security context is established.	Comments: This method is potentially vulnerable to spoofing attacks such as SIM-Swap fraud.

Security mechanisms for RCS clients		
	Open ID Connect (OID): This method is utilised when RCS service provider extends a security context to interfaces using HTTP as access protocol.	
Encryption	RCS clients can utilise TLS and IPSec where available to ensure confidentiality of communications. This security measure would protect consumer’s privacy.	Comments: End-to-end confidentiality may not be guaranteed due to lack of support for TLS and IPSec beyond the access network across transit. A bespoke secure channel between RCS client and service maybe required for realising confidentiality and integrity of information exchanged
Storage of Authentication and Identification Data	The RCS client is required to store authentication and identification data in a secure manner. This measure is to protect consumer’s data and access to RCS service.	Comments: The potential risk here is compromise of integrity of the underlying mobile OS. The data must not be stored on removable storage in plaintext. Robust tamper detection mechanism is required to ensure sensitive data is not exposed if the OS is compromised (e.g. Root access in Android). Adequate storage is needed such as SIM or embedded SE or in mobile OS platform features such as Android KeyStore with a hardware backed TEE or a bespoke secure container ensuring confidentiality and integrity of data stored.
SIM State Handling	If identification and authentication of RCS client is based on SIM Ready State then in a not Ready State (powered off, physically removed) RCS must invalidate all existing security context.	

Security mechanisms for RCS clients		
Client Authenticity	The procedures to allow a HTTP Configuration Server to verify the authenticity of the client requesting to be configured are defined in GSMA specifications[20]. However, this aspect is under development for RCS clients running on Android O/S.	

D. Potential Risks in using SMS as a Data Bearer for OTP

Potential risk	**Severity**	**Description**	**Potential impact**
Fraudulent SIM replacement (also known as SIM-Swap or SIM-Jacking) or Unauthorised Number Porting	High	Fraudsters use social engineering techniques to convince MNO staff to order a replacement SIM with the same MSISDN delivered to a new address, or they impersonate a legitimate consumer to setup a new account and port the victim's MSISDN to fraudster's SIM. These lead to an effective account takeover scenario and can compromise payment transactions relying on OTP delivered over SMS. The attackers typically would use this technique after compromising the basic authentication (username and password) and want to retrieve the SMS based OTP to complete a transaction. With a new SIM and the original MSISDN in place attackers can receive the required OTP over SMS and complete the transaction. By the time the legitimate consumer becomes aware of this, fraud would have occurred with potential monetary loss.	• Account takeover • Monetary loss

[20] In GSMA PRD RCC.14 Service Provider Device Configuration, version 5.0, 28 June 2017

Potential risk	**Severity**	**Description**	**Potential impact**
SMS Re-routing exploiting SS7 vulnerability	Medium	Signalling System 7 (SS7) is used for exchanging data between network appliances used in mobile telecommunication networks. The signalling messages related to a mobile subscriber do not guarantee origin authenticity on their own, and it needs an additional check to determine if the subscriber is located within the network from where the signal originated. Attackers exploiting vulnerabilities in SS7 can potentially re-route and access SMS with OTP and complete a payment transaction.	• Account takeover • Monetary loss
Malware	Low	Malicious software on mobile phones can potential retrieve SMSs with OTP and redirect to fraudsters.	• Account takeover • Monetary loss
Phishing	Low	A legitimate consumer may be redirected to a fake website via phishing message. The attacker then relays the basic authentication details received from consumer to the legitimate service provider. The consumer receives OTP in SMS from legitimate service provider which is then presented to fake website. The attacker can then use that OTP to access the consumer’s account or complete a transaction	• Account takeover • Monetary loss
Lack of confidentiality of SMS	Low	SMSs are not necessarily encrypted end-to-end when transferred across the mobile telecommunication networks. SMSs can also be stored as plaintext in Short Message Service Centre (SMSC) before delivery to the intended recipient. Any security compromise of mobile network including SMSC due to malware or rogue personnel can lead to potential disclosure of OTPs in SMS	• Account takeover • Monetary loss

Potential risk	**Severity**	**Description**	**Potential impact**
Delayed delivery	Low	SMS with OTP getting delivered in a delayed manner. This can be due to network congestion. The occurrence of this is more during holiday periods and locations with high population density and scarce mobile network services.	• Transaction getting timed-out and failed • Diminished consumer experience • Monetary loss due to abandonment
Delayed presentation to consumer	Low	With not enough memory available in the mobile phone the SMS with OTP may not be available for the consumer	• Transaction getting timed-out and failed • Diminished consumer experience • Monetary loss due to abandonment

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London
EC4N 8AF
United Kingdom
www.gsma.com