Connected cars are one of the earliest connected objects to be augmented with payment capabilities. This paper exposes the variety of use-cases related to connected vehicle payment, and reviews the challenges and limitations with respect to technologies and regulation. The industry is already at work building proprietary approaches and Big Tech actors are pushing forward while trying to make the most of their assets. We recommend promoting interoperable solutions based on common standards, including 5G technologies, and capitalizing on existing and upcoming European payment methods (SEPA Request-to-pay, EPI...).

I. FOREWORDS

We explored in [1] (appended in annex) the general topic of connected object payment: from proprietary approaches to an open, interoperable paradigm, we outlined some strategic challenges and exposed how existing schemes and regulations could evolve toward including IoTs capable of making partially or fully autonomous financial operations.

Building upon this work, the present paper focuses on cars (and trucks), a class of connected objects which has gathered considerable attention around the world in recent years. Notably, a number of experiments have already been conducted with respect to vehicle payment, and the entire automotive ecosystem is currently organizing itself around innovative solutions and new use cases, making cars among the earliest connected objects to get actual payment capabilities.

After an introduction below, we explore in section III the variety of use-cases dealing with vehicle payments. It provides a reading grid to address technology enablers and challenges in section IV, and the regulatory framework in section V. Finally, section VI offers some recommendations.

II. INTRODUCTION

The era of the connected car is here... With about 75% of new cars delivered in 2020 having embedded connectivity, more than 250 million vehicles globally are already equipped with some kind of network attachment, enabling a variety of innovative services. Among them, payment is sparking considerable interest: Early experiments as soon as 2015 began to explore usage around gas refill, parking and toll fares. Since then, there has been an abundance of explorations from actors as diverse as car manufacturers, the petroleum industry, insurance companies, bank and non-bank PSPs, card schemes, fintech startups, telcos, and even restaurant chains. Today, the profusion and variety of use cases are unquestionable, as are business opportunities. Worldwide commuters spend an excess of $200 billion a year conducting commerce in their cars with their smartphones [3], and two thirds of them are willing to shop more frequently provided in-car purchasing integration and payment were available. Gartner [4] forecasts in-vehicle payments will total one billion dollars by 2023, up from less than $100 million in 2020, mainly on fuel, food or parking.

To this day, the multitude of implementations is driven by big players, mainly from the USA, mainly in siloed, proprietary approaches. They have few expectations towards regulation or interoperability, but rather conduct pragmatic investigations.

III. A VARIETY OF USE-CASES

Situations where a user pays with a mobile phone or a smart watch are relatively simple ones. This is because the connected object is privately owned by a single user. By contrast, situations where the payment is mediated by a vehicle are more diverse, as the ownership of the vehicle and of the payment method can be combined (figure 1).

Figure 1. Use-cases with respect to payment method
A vehicle can be privately owned and used. In this case, the payment method (personal or professional) can be provided by the owner, the driver (e.g. when the car is shared between family members), a passenger, or even several people if carpooling. But it could also come from a third-party service provider. For instance, the car manufacturer may bundle a payment service with its financing offering (e.g. a credit contract including the provision of a dedicated bank card token, or even a GAFA payment method, to be used for the duration of the credit). otherwise, an applicative service (e.g. bill splitting) could provide a dedicated tokenized card to be added to the vehicle wallet.

If the vehicle is shared, rented or leased, the end-user can provide a token for their payment method (personal or professional) as well. In addition, the rental or leasing firm may elect to offer a supplementary payment service, with the provision of a dedicated token already active in the rented/leased car.

Finally, the vehicle can belong to a corporate fleet. Evolution to current fleet management services, which sometimes already manage customized fuel cards, could allow for payment methods provided by the end-user, by a financing/rental service, or by the company (having the fleet) itself.

There are also differences between use-cases involving vehicle-to-merchant interactions (gas station, parking operator...) and in-vehicle purchases or consumption. Depending on the nature of the transaction, it may be initiated by the consumer (CIT), e.g. for online ordering, by the merchant (MIT) for delegated payments, or even by the vehicle (OIT, see [1]) for autonomous or semi-autonomous transactions. Every situation described above has different constraints with respect to regulation and liability, as we will see in section V.

Figure 2. Use-case: electric vehicles recharge

Figures 2 and 3 depict two examples of use-cases (with additional illustrations provided in annexes). In the first one, a professional end-user needs to recharge their professional/fleet electric vehicle (fig. 2). Upon arrival at the facility, the car enters a pairing agreement with the charging infrastructure, and a transaction is started after the user plugs the charging cord and validates a screen on the car console. The payment transaction is terminated when the charge is complete. The second example (fig. 3) presents a personal use-case, where an end-user interacts with a drive-in service through their car (hosting a payment method), with similar steps (and console illustrations in annexes).

In both examples, several operations are ideally performed (e.g. wireless telecom pairing), but they can raise some technical challenges in the real world.

IV. Technology Enablers

Enabling vehicle payments in an open environment raises several challenging technological issues. It is a somewhat more complex operation than just tapping a bank card or a mobile phone on top of an electronic payment terminal (contactless payment), as some secure mid-range pairing is required. An actual payment scheme can then be used, with software components within the vehicle supported by an embedded operating system.

A first challenge is to set up a secure communication channel between a vehicle and the merchant infrastructure. Several technological approaches can be considered, and they can be classified into two broad approaches: technologies that are generally available, hereafter denoted as "best-effort", or managed technologies providing tailored services, offered by operators.

Best-effort solutions include wireless capabilities such as Bluetooth (with BT advertising) or WiFi (with WiFi Direct) to build up a digital link, onto which secure communication can be set up using classical Internet security mechanisms. These assets are potentially easily available, allowing for quick deployment. On the other hand, they can provide subpar security, and give Big Tech actors a strong hold on vehicle payment.

Managed solutions include the 5G Device To Device and 5G Proximity Services offering, essentially providing Machine to Machine connectivity with good scalability and strong security. A strong identity scheme is also available thanks to the inherent security of the e-SIM to provide cellular network-enabled authentication. Another strength of managed technologies is their scalability, allowing consistent service under high capacity requirements. However, these technologies require more time before they are deployed and widely available. Vehicle payment is clearly an innovative use-case for 5G in Europe, which should be more thoroughly investigated.
The next operation is the payment initiation. An analogy to the tapping gesture must be implemented, requiring some innovation, potentially based on localization, in order to assess an “intent to pay” (for instance Ultra-Wideband, operating at GHz frequencies, and RTK GPS – real-time kinematic satellite positioning, providing centimeter accuracy – are candidate technologies).

The last step is about the actual payment transaction, conducted using standard schemes such as EMV or PSD2 protocols. Provided adequate security is reached by the previous network layers, there is no technological issue in this regard. Other opportunities are the upcoming European Payment Initiative (EPI) [5] and the SEPA Request To Pay (RTP) [6] schemes, which should be designed in a manner compatible with such a transaction.

Another significant enabler is the automotive operating system. While current vehicles still embed proprietary software, there is a heavy trend for OEMs to adopt Android Automotive OS [7] in the short term. This open-source package by Google seems well suited to vehicle payments: not only it is a security model in line with payment requirements (sandboxing, secure inter-process communication), but the Google Pay service is compatible with the automotive OS, making straightforward the provision of a vehicle wallet. However it should allow third parties to implement their own wallets, as it is currently expected by the EU commission for mobile phone wallets [2, 8]. Furthermore, the Android Automotive OS provides advanced identity management, with potential user recognition and profile switching, making it possible to implement all kinds of use-cases.

Other automotive OS and more generally IoT OS will likely also develop payment support features, which should be made open to third parties in the same manner.

V. REGULATORY FRAMEWORK

With respect to payment regulations (such as the European PSD2) and existing standards and rules applicable to different payment instruments, the situation is somewhat different, with some use-cases being properly covered by existing regulations while others lack a consistent framework and call for regulatory change in the longer term.

A first category of use-cases involves a single user bringing their own payment method, tokenized into the wallet of the vehicle. This is typically a customer initiated transaction or CIT. Since no special provision is made for IoTs within the regulation, the general rule (related to consumers) comes into play. The PSD2/RTS framework requires that strong customer authentication be applied to a transaction (by verifying two factors among three, namely knowledge, possession and inherence). This is, however, subject to exemptions: examples include when the amount is less than thirty Euros, when the merchant is listed as a trusted beneficiary, and/or specific businesses/verticals. A two-factor authentication involving the car systems can be designed, for instance combining driver recognition mechanisms (digital key, face recognition...) with the input of a secret code.

Another approach could be a merchant initiated transaction (MIT), involving a payment using SEPA Direct Debit (SDD). Following the initial setup of a SDD mandate, there is no need for strong authentication on further transactions. Obviously, the requirement to set up such a mandate in the first place restricts the usefulness of such a payment method to recurring purchases and regular merchants.

All other use-cases are more challenging, as they are not covered by PSD2 or the payment scheme rules. This includes situations in which the owner of the payment method is not present: shared vehicles, payment method provided by the car rental firm or even embedded by the car manufacturer.

An alternative is to consider professional bank cards, which are not fully within the scope of the PSD2, but are rather regulated by card schemes. For instance, current lodged cards make possible non-authenticated purchases on behalf of a corporation, usually restricted to accommodation expenses. An evolution of this principle could allow other kinds of non-authenticated purchases on behalf of the car rental firm. Alternatively, since the payment method is a dematerialized one, an innovative issuer could provide on-demand digital business bank cards, in the name of the driver, on behalf of the rental firm, uploaded in real-time as a token inside the wallet of the car.

Using professional bank cards thus seems a viable way for actors to innovate and, at least, deploy proofs of concept and pilots. It should be stressed out that these cards are not subject to interchange limitations of the PSD2, and thus may be more profitable for issuers. This is a clear incentive to investigate vehicle payments, where an added risk may be compensated by higher revenues. It should also be noted that this payment process would build on unclear legal rules and therefore may be subject to regulatory change in the near future.
Another alternative is to embed the payment method within the vehicle. By analogy with the e-SIM card currently concealed by manufacturers of connected cars, it is indeed possible for OEMs to preload a card token or another payment method. Alternatively, big players could implement privative architectures using electronic money or even cryptocurrencies. By contrast, an open and interoperable solution would require the evolution of the applicable regulations, as we outlined in the previous memo [1].

VI. CONCLUSION

It is clear from the above analysis that some innovation is still required for connected vehicle payment to become commonplace. Alternatives to let industry actors innovate on their own, or to have public authorities steer innovation toward some standardization allowing for an interoperable, open approach.

On the technical side, 5G innovation around payment use-cases should be encouraged. The dependence of the industry on automotive operating systems will increase in the short term, and we can expect object wallets to naturally fall into the hands of Big Tech actors. In the same timeframe, the regulatory framework will not significantly evolve, pushing industry actors to adopt ingenious solutions in order to make the most of existing provisions (e.g. test professional card payment to avoid strong customer authentication rules).

We therefore recommend some vigilance with respect to wallet openness, the role of GAFA and in general sovereignty, including applications to the future EPI and RTP payment methods, which should be designed from the ground up to encompass such innovative use-cases. To quote the European Commission strategy in [2], it is desirable to "(...) develop and offer to all European users, without undue restrictions, innovative payment solutions using all relevant technical infrastructures, under fair, reasonable and non-discriminatory terms and access conditions". As much as this was likely written with online and mobile payments in mind, this must be envisioned for IoT and vehicle payments as well.

The scope can even be broadened to embrace mobility solutions, where multiple travel modalities can be combined and paid for in a single transaction. We must also keep in mind longer term use-cases, where IoTs exhibit fully autonomous payment capabilities, requiring new rules and regulation, as we outlined in [1].

ACKNOWLEDGMENT

This work was conducted under the GTS working group, sponsored by the Comité National des Paiements Scripturaux, and co-chaired by the Direction Générale du Trésor and the Association du Paiement. Contributors to this work include Michael Pontiggia (Orange), Sophie Allain Des Beauxais (Banque de France), Benoît Ouinas (Netcetera), Florence Chen (Crédit Mutuel) and Colombe Hérault (Worldline).
ANNEXES

Use-case 1: fleet vehicle recharging

Use-case 2: personal car drive-in order

Fleet vehicle / pairing information

Personal vehicle / entry into the queue

Fleet vehicle / start of transaction

Personal vehicle / payment transaction

Fleet vehicle / end of transaction

Personal vehicle / payment terminated
Adapting payment to the Internet of Things

François Toutain, Emmanuel Le Huérou (Orange), Pierre Françon (Quaelys)
François-Xavier Lecarpentier (Orange), Benoît Ouinas (Netcetera)
Dalila Hattab, Sylvie Calsacy (Worldline)
May 2020

This paper explores what it means for connected objects in a B2C context to be able to initiate payments, from devices which only act as triggers in closed solution approaches, to an open, interoperable paradigm which can be embodied in the context of the European Payment Service Directive number 2 as well as in the card schemes and upcoming payment methods. Strategic challenges are exposed, and the evolution of the value chain is made clear, giving rise to some initial recommendations.

I. INTRODUCTION

The last few years have seen the emergence of a multitude of payment initiatives, with new actors promoting privative solutions, and also innovation around open four-corner approaches, including the European Payment Initiative. But the underlying model is still always based on a user mastering the payment or delegating it to a merchant. Meanwhile, recent advances with connected objects - the so-called Internet of Things - make it now possible to envision a new model where objects are able to make autonomous payment actions.

In the following, we focus on consumer objects and use-cases, even if merchant devices, initiating unattended transactions, could also be considered and would require further study.

II. IoT

The Internet of Things can be defined as the interconnection of devices within the existing Internet infrastructure, providing advanced connectivity of devices, systems and services beyond machine-to-machine communication [1]. Application domains range from Industry, Agriculture, Logistics, to Telemedicine, Commerce or Smart Home, with forecasts of billions of connected devices in the coming years. Among these objects, only a subset can be expected to be involved into payment actions, with likely use cases related to wearable devices, command interfaces (e.g. smart speakers), sensors for online services (e.g. smart fridge), and also connected vehicles and connected locations [4, 5].

IoT devices fundamentally require suitable communication modes. These channels are ideally provided by an infrastructure such as 5G mobile networks, which were partly designed for this kind of usage.

III. IoT AS A PAYMENT TRIGGER

In a number of current solutions, a dedicated device is integrated in the service chain requiring payment. Consider for instance a proprietary electronic toll collection service. The subscriber receives a device to be displayed behind his vehicle windshield. When a toll collection gate is crossed, some wireless interaction is initiated to trigger the payment. In a way, the device is thus the trigger of the payment transaction. However, the payment instrument is held by the service back office and not by the device itself. This implies a prior subscription, since the user had to provide their payment method beforehand. This is a well-known paradigm: in such an account-based solution, the payment can be processed (1) as a Merchant Initiated Transaction (MIT) if the user is not in a position to authenticate the payment in a timely manner (such as toll), or (2) as the traditional Consumer Initiated Transaction (CIT) way.

The current market trend is towards such a privative approach, favoring big players and market leaders, and making it almost impossible for alternative actors to emerge, as there cannot be any interoperability in this context [2, 3, 6]. Among these big actors, GAFAM and BATX are already active in both the IoT and payment domains.

IV. IoT AS A PAYMENT TRANSACTION INITIATOR

Another paradigm can be envisioned, where connected objects are able to hold a payment method, and are able to initiate a payment on their own, with or without a user interaction. In this approach, any actor can be a part of an interoperable infrastructure, including device manufacturers, service providers, third-party payment providers, merchants...
A. Use-cases

In an elaborate Vehicle to Infrastructure (V2I) scenario (figure 1), a connected car is able to initiate a payment required by a merchant, with either an automaton (gas distribution, toll collection, car park terminal) - via an unattended transaction, or a human employee - via an attended transaction. The car must be within range of the merchant acceptance point, via a secured payment communication protocol.

The car embeds a secure o-wallet (object wallet) allowing the owner or the user to enroll their payment method: card, IBAN or any kind of payment token. The holder of this payment method may delegate to the car itself a right to autonomously initiate payments; it may also possibly require a confirmation step for each payment (consent and relevant proof).

Similar use-cases can be applicable in the context of vacation rentals or dependent persons, with different connected devices – two examples are described in the annex.

In terms of user experience, the benefits are straightforward as a user can enjoy any compatible service accessible through the connected object, thanks to an open payment system with no prior enrollment required. Reuse and sharing are also facilitated among users, since any user can set their payment method onto the device for a limited time.

B. New concepts

By contrast with classical CIT and MIT methods, the object is now able to autonomously initiate a payment, thus an Object Initiated Transaction (OIT) model is at play. Nevertheless, in such a model, it may not be possible to authenticate the owner of the payment method (they may not be present, or may not have access to an authentication interface, or may not be able to react in real time). Yet the merchant is not initiating the payment, the connected object is.

As a consequence, a delegation mechanism is required, as well as a way to ensure that a paying device actually received a prior delegation from the owner of the payment method, in a kind of object authentication. In the next two sections, we review how such concepts can be integrated into a PSD2 architecture and into an EMVCo model.

C. In the context of PSD2

In the philosophy of the European Payment Service Directive 2 (PSD2), banks (ASPSP) are ultimately responsible for ensuring a secure payment initiation, with a Strong Customer Authentication (SCA). An OIT model can thus be implemented by (figure 2):

- a delegation step where the user (authenticated with SCA) provides an object identifier, used by the ASPSP to communicate with the object and set up a way to authenticate it,
- a modified payment initiation cinematic, where the ASPSP authenticates the object (fully autonomous payment request) or the user (user initiated, object mediated payment request),
- and possibly by defining new exemption rules.

This approach places a considerable burden on ASPSP to handle object identities and authentication. Banks may not be the ideal players to manage millions of technical transactions. An alternative could be to define a new kind of third-party actor, namely the Object Payment Initiation Service Provider (OPISP). This role would encompass the...
classical PISP role, with additional capabilities to manage delegation, object lifecycle (enrollment, authentication and repudiation), and possibly user authentication or consent via the object interfaces or via a remote one (figure 3).

D. In the context of EMV-based payments

In card schemes, a CIT model involves a Cardholder Verification Method (CVM) authentication for a face-to-face transaction or an EMV® 3DSecure one or remote payment. Merchant initiated transactions are usually conducted with no real-time authentication (Card On File), but a decoupled authentication was recently proposed by EMVCo, where the verification can be performed separately from the payment. The new OIT model can be implemented with such an approach, if tokenization is deployed, providing tight control of the device allowed to make use of the tokenized PAN (figure 4). In summary, the Payment Networks specifications of HCE (Host Card Emulation) and 3D Secure provide one possible technological answer to the OIT model. In addition, Consumer Device-CVM (CDCVM) allows for cardholder verification through the device interfaces.

E. New payment infrastructures

Other innovative payment infrastructures are currently under study, including Distributed Ledger Technology (DLT). DLT can be applied to the provision of Central Bank Digital Currency (CBDC), and the resulting payment system is not necessarily conflicting with PSD2 objectives. The opportunity to implement the OIT model will have to be taken into account in such studies. The processing time for such implementation is to be assessed, as well as the Object Authentication mechanisms.

F. How mobile network (and 5G in particular) can be an enabler

A number of mobile technologies are promising assets in the context of IoT payment: device identity is managed through eSIM (embedded Subscriber Identity Module), providing a certified and authenticable identity; Machine to machine communication protocols offer suitable quality of service to e.g. vehicle infrastructure; medium range secure radio communication could serve as an enabler for dedicated payment protocols, for all contexts including DSP2, EMV, or new payment infrastructures.

Current 4G networks can already provide some of these assets. However, 5G, the upcoming technology standard for cellular networks, aims at improving smartphone data speed (i.e. Enhanced Mobile Broadband), but it also encompasses a diversity of additional service levels, from Ultra Reliable Low-Latency Communications to Massive Machine-Type Communication which could really benefit IoT payment.

For example, Network slicing is a structuring concept of 5G (figure 5) [7]. It enables service providers to build virtual end-to-end networks tailored to application requirements. A network slice dedicated to IoT payment could be studied, and could be jointly designed by the European Commission and the GSMA, as a standard to be implemented and operated by all telecom providers.

V. STRATEGIC CHALLENGES

A number of key issues are raised in this context. Integrating and possibly adapting the EPI is an important one, as future IoT payment usages could greatly benefit from this new payment mechanism. The PSD2 directive can also accommodate these usages, with some evolution. It is anyway of prime importance to design interoperable systems, to open the market and avoid the dominance of a few global players. Such a move could be facilitated by a common technical infrastructure provided by 5G technologies, including as an EMV communication protocol.

Security issues linked to the IoT are also an important stake. A number of current devices and services are well known to have been marketed with scant regard for security, providing easy targets to hackers. Introducing payment capabilities in this ecosystem calls for more stringent security requirements. Personal data are also at risk and require that the GDPR be strictly enforced.

In summary, IoT payment is an emerging field conducive to the affirmation of European strategic independence.
VI. CONCLUSION

The conjunction of IoT and payment triggers **evolution in the value chain**. Where we had customers, merchants, and third-party enablers facilitating payment, we now have connected objects and a layer of actors implementing end-to-end payment: incumbents sticking to their usual role (e.g. banks), existing players evolving toward a new role (e.g. telecom providers, payment processors), and maybe new actors such as dedicated IoT payment Fintech. Also **big digital players** (i.e. GAFAM and BATX) **must be closely monitored**, as they already operate on the domains of IoT and payment.

Some initial recommendations could include **encouraging 5G technologies** in IoT payment infrastructures to secure M2M exchanges. Moreover, it is **crucial to favor universal approaches**, e.g. by promoting a generic model, to be implemented on all open payment ecosystems (four corner card/token, DSP2, DLT/CBDC). This would foster competition and prevent this emerging market from being locked up by a few key players.

ACKNOWLEDGMENT

This work was conducted under the GT5 working group, sponsored by the Comité National des Paiements Scripturaux, and co-chaired by the Direction Générale du Trésor and the Association du Paiement. Contributors to this work include Orange Labs, Quaelys, Netcetera, and Worldline.

REFERENCES


GLOSSARY

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASPSP</td>
<td>Account Servicing Payment Service Provider</td>
</tr>
<tr>
<td>BATX</td>
<td>Baidu, Alibaba, Tencent, Xiaomi</td>
</tr>
<tr>
<td>CBDC</td>
<td>Central Bank Digital Currency</td>
</tr>
<tr>
<td>CIT</td>
<td>Customer Initiated Transaction</td>
</tr>
<tr>
<td>CVM</td>
<td>Cardholder Verification Model</td>
</tr>
<tr>
<td>DLT</td>
<td>Distributed Ledger Technology</td>
</tr>
<tr>
<td>EMV</td>
<td>Europay Mastercard Visa</td>
</tr>
<tr>
<td>EPI</td>
<td>European Payment Initiative</td>
</tr>
<tr>
<td>eSIM</td>
<td>Embedded Subscriber Identity Module</td>
</tr>
<tr>
<td>GAFAM</td>
<td>Google, Apple, Facebook, Amazon, Microsoft</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>GSMA</td>
<td>Global System for Mobile communication Association</td>
</tr>
<tr>
<td>HCE</td>
<td>Host Card Emulation</td>
</tr>
<tr>
<td>IBAN</td>
<td>International Bank Account Number</td>
</tr>
<tr>
<td>M2M</td>
<td>Machine to Machine</td>
</tr>
<tr>
<td>MIT</td>
<td>Merchant Initiated Transaction</td>
</tr>
<tr>
<td>OIT</td>
<td>Object Initiated Transaction</td>
</tr>
<tr>
<td>OPISP</td>
<td>Object Payment Initiation Service Provider</td>
</tr>
<tr>
<td>PAN</td>
<td>Primary Account Number</td>
</tr>
<tr>
<td>PISP</td>
<td>Payment Initiation Service Provider</td>
</tr>
<tr>
<td>PSD2</td>
<td>Payment Service Directive 2</td>
</tr>
<tr>
<td>PSU</td>
<td>Payment Service User</td>
</tr>
<tr>
<td>SOA</td>
<td>Strong Object Authentication</td>
</tr>
<tr>
<td>SCA</td>
<td>Strong Customer Authentication</td>
</tr>
<tr>
<td>V2I</td>
<td>Vehicle to Infrastructure</td>
</tr>
</tbody>
</table>

CONTACTS

emmanuel.lehuerou@orange.com
francois.toutain@orange.com
pierre.francon@quaelys.com
francoisxavier.learcaptopier@orange.com
benoit.ouinas@netcetera.com
dalila.hattab@equensworldline.com
sylvie.calsacy@worldline.com

ANEXES

Annex 1. Use-case: wearables in the smart city

Annex 2. Use-case: location rental/sharing