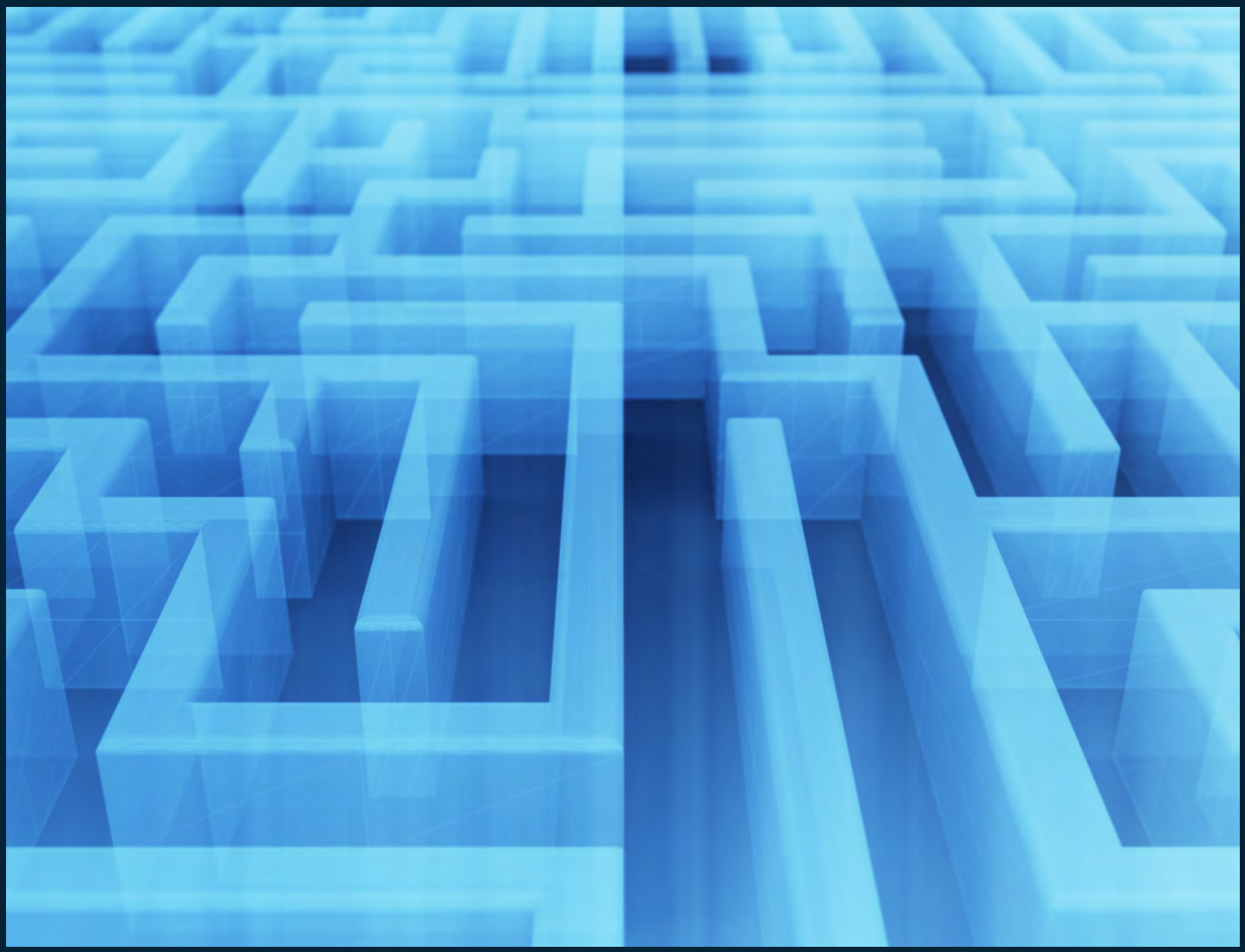
TRUSTONIC

FAQs
In-vehicle payments Webinar

18 Qs



Contents

Standards & Regulation

Question 1:

As the group is talking about the rise of IoT payments and connected vehicle payments, why does it feel like the Payment Services Directive 2 (PSD2) regulations kind of left out this specific categories and focused for the most part on the smartphone as the "major" mobile payment device - or did I just miss this part?

It is fair to say that PSD2 was not originally designed for automotive. On the other hand, as a standard, it's quite technology and payment channel agnostic. What it provides is a framework for how to integrate the required components. For a vehicle, you can think about biometrics or potentially even something like PIN as a first factor, and then a secure key / a cryptographic key, or credential as a second factor. Ultimately, it will be down to the issuer (the OEM or a bank for example) to decide on the specific set of authentication mechanisms, that are required taking into account PSD2 and related Strong Customer Authentication (SCA) requirements.

Question 2:

Next generation connected vehicles may be required to process credit card information, do you think any such processing requires separate vehicle level certifications /audit for PCI-DSS in future just like cloud and other on-premise infra?

You have to start by looking at the technology being used to provide the security for the solution. It is a secure element, either a Trusted Execution Environment or a cloud-based payment solution.

Based on the technology path chosen, there are different requirements and certifications. Many of these will be managed by the technology provider who will pre-certify the hardware and software. The technology solution should not be an additional burden on the vehicle manufacturer, as they will inherit the certification compliance.

There will of course be a need to plan for the long term, so that the full lifecycle of the vehicle is considered.

For example, at Trustonic we have started an EAL 5 certification process which is a higher level of certification than is currently being requested. We are taking this step. We want to ensure that our Trusted Execution Environment is suitable for the whole vehicle lifecycle.

It is also worth noting that another option for the in-vehicle part could be to restrict the vehicles role to authentication only (hosting authentication credentials). Using this approach, the vehicle would not store the card data within the vehicle itself. The combination of card tokenisation (for e-commerce) and delegated authentication could help to remove the need for the OEM to obtain PCI certification of its model range supporting in-vehicle payments.

Question 3:

How does In-Vehicle payment impact UNECE WP.29 automotive cybersecurity regulation?

The new UNECE WP.29 on Over the Air Software Updates and uniform provisions represents a major change for the auto industry. These regulations focus on the approval of vehicles with regards to cybersecurity and cybersecurity management system. These new regulations will require OEMs to include specific cyber security capabilities and mitigation in the vehicles. They also specify that operating Security Operation Centers should be able to monitor and detect emerging threats against vehicles.

The capabilities required by the new WP.29 regulations will provide a core foundation for the security that will be required to deliver In-Vehicle Payments.

Question 4:

There doesn't seem to be any regulations related to embedded cameras in-vehicle in order to allow PSD2 compliant transactions. How can an OEM make sure that their camera is sufficiently secure for in-vehicle payments with facial authentication?

Today, card issuers decide which authentication methods are secure to allow for PSD2 compliant transactions. Therefore, an OEM needs to work with a card issuer to agree on a certification standard and process with potential bio-authentication solutions.

Technology

Question 5:

In-vehicle payment model increases the vehicle cost drastically, e.g. to support plug & charge feature it involves huge effort of cybersecurity implementation, electronic changes, etc. How do you think it will go?

Today, there are already many wireless technologies that are integrated into a vehicle for a range of different applications and scenarios; everything from digital car keys to eCall support to streaming content services.

There are also new general cybersecurity requirements such as UNECE WP.29 and new ISO requirements such as 21434. These will also require vehicles to embrace cybersecurity into the heart of the vehicle design process.

This will by default provide the secure route of trust and the secure environments inside the vehicle that naturally enable payment transaction services to be protected. This will be done in a robust way, that meets the needs of the financial services industry. In addition, a range of countries around the world, are also introducing driver monitoring and sensing systems that can also be leveraged to support user authentication.

The direct cost for OEMs to support the enabling technology will be relatively low. This is due to the core components, such as a hardware root of trust, two factor authentication type services, have to be deployed, in order to meet regulatory compliance and general consumer experience requirements.

Finally, in-vehicle payments should also be a platform for revenue generation for the OEM. The cost of implementing these solutions should be more than offset by the potential to generate revenue across the lifetime of the vehicle.

Question 6:

When everyone in the car carries a smartphone, which can make any payment , does in vehicle payment make any sense?

There are several aspects to this question:
Firstly, it's likely that a vehicle user will have a combination of payment solutions. A kind of omni-channel that enables them to use different form factors, different services from the same account or wallet.

Thus, it's likely to be a situation or a credit card number, but it depends on the situation where you use a certain payment or solution.

Another consideration is that using a phone in a vehicle is against the law in many countries and is considered a major source of driver distraction. Therefore, there is a big benefit by enhancing safety, and avoiding the need for the driver to take their eyes off the road.

Question 7:

Is digital money the ultimate solution for in-vehicle payments? Such as the work G+D and Worldline is doing?

There are several payment mechanisms that can be used for in-vehicle payments such as: credit card, direct account-to-account and digital currency. The success of a chosen payment method depends on the endorsement of the ecosystems and the user experience.

Another aspect to consider is the Nx1 identification between driver and vehicle. In a car-sharing scenario there is more than one driver driving a vehicle. It is true that the link between user identify and car identity is crucial. Moreover, in many cases, the user wants to be anonymous.

Question 8:

The vehicles by their nature have a long life, where next generation electronics and mechanical may not go hand in hand. With In-Vehicle payment support, how do we anticipate upgrade issues due to cybersecurity attacks. E.g. upgrading crypto algorithms in TEE/SHE and inbuilt cryptographic keys specially when standards (EMV/X9 etc) keep on upgrading, but the vehicle may require whole ECU electronic upgrade?

Clearly moving forwards it will be very important to keep vehicle software up to date and to provide the highest level of protection possible. With new regulations such as the updates to UNECE WP.29 and ISO 21434 a strong focus is being placed on the ability to keep software platforms inside the vehicle "ever green". You have also highlighted the use of a TEE as part of the AUTOSAR SHE architecture. One of the benefits of using a TEE to provide the key storage and cryptographic support within AUTOSAR is its ability to be securely, remotely updated to support new keys and cryptographic algorithms.

Question 9:

Why can't a headunit be developed in such a way that accepts a simple iPad fitment, similar to the bring your own device concept and development cost is lower?

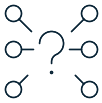
There is no reason why an OEM or Tier 1 could not design a solution that supports the vehicle user using their own tablet. With CarPlay and Android Auto the screen mirroring solutions to enable the tablet to work as part of the IVI experience, are already in place also with support for specific automotive modes on the tablets themselves.

Question 10:

Any view on how to improve the "biometrics", is voice next?

There are a wide range of biometric options now becoming available. These include Iris recognition, voice print matching, and steering wheel mounted sensors, so that you do not need to remove your hands from the steering wheel in order to authenticate. It is likely that we will see multiple biometric sensors being used to authenticate drivers moving forwards to provide the strong level of authentication possible.

There have also been strong advances in driver fingerprinting using multiple inputs, such as seat pressure sensors, seat position, driving style (for example how hard do you press the pedals), temperature settings, audio volume etc … These can also be used to help further validate who is driving the vehicle.



Question 11:

Can driver behaviour be used as Identity?

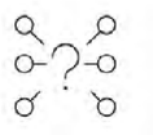
Potentially yes. Driver profiles can differentiate between different drivers,but they aren't strong enough for authentication. For example, a basic system might identify between drivers depending on which key they use, whereas a more advanced system might use a camera to recognize the driver. However, in both cases the focus is on selecting the driver from a very small set of users rather than true authentication.

That said in future there is no reason in principle why technology such as a camera added to a car for driver recognition or driver alertness monitoring could not also be used for facial recognition.

Question 12:

How to you see authorization for payments in car, imagine that the driver is alone and driving at 130k/h ?

The previous answers have outlined a number of different biometric technologies that can be leveraged to support payment authorization. For the use case given above, it would be critical that an authentication solution is used that does not create driver distraction, or require them to take their eyes away from the road. Good examples of such solutions could include Voice biometrics or steering wheel mounted fingerprint or palm print readers.



Question 13:

Is the car becoming a wallet, or will the owner have a wallet that will have to sync with the car?

It is highly likely that the vehicle will become a wallet over time, as in-vehicle payment capabilities become common within the automotive industry. You can already see today that Google wallet has already become part of the vocabulary in the automotive industry.

In-car payments will likely have an impact on server payment models. There are three clear long term alternatives:

- Credit card schemes, with tokenisation.
- Direct account payment.
- Blockchain technology, where we expect to see a lot of innovation moving forwards.

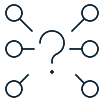
Today we are seeing a lot of companies experimenting and learning as they develop their plans, but we are some way from the industry having a fully standardized approach.

It is also good to look at from a product perspective, because once you have an OEM pay platform established for the vehicle, that will be one of the payment channels. However, it is highly likely that we will see other channels coexisting. Like the mobile industry, where OEM schemes co-exist with traditional and web-based payment schemes.

Ultimately, it's about the drivers' identity being connected to payment identity and payment credentials. This also presents usability challenges when you take all the challenges, not only in the car, but also in the mobile and in the wallet.

There needs to be a harmonized experience, especially when considering transferring your identities, your credentials from one channel to the other, using both in parallel are using maybe one of them only temporarily and so on.

Viewing this as a product ecosystem, where you will have a classical mobile wallet, maybe also with the OEM branded, payment cards, an HCE wallet, for example, with your mobile phone. In addition, you will also have the in-car wallet and maybe also a web-based wallet. Hence, it's a really a complete consumer ecosystem and how you integrate into that and not an isolated solution.



Question 14:

How will in-vehicle payments work in self driving cars ?

It is maybe too early to say how in-vehicle payments will change with full autonomous vehicles, but in principle, if the driver does not need to be focused on the road, then the vehicle provides for a wider range of authentication and verification solutions to be utilised.

Question 15:

Where do we see this "In-Vehicle Payments" more focused - Commercial vehicles vs Personal vehicles?

In-Vehicle payment solutions will be focused on both consumer and commercial vehicles, but are likely to target different use cases and customer benefits. Many of the early trials for in-vehicle payments have focused on both consumer and commercial vehicles.

Question 16:

What automotive brands are already on board? Or have been trialing the technology?

There have been many trails over the last few years.

- Some of the public ones include:
- Honda and Visa (2018)
- General Motors and Shell (2018)
- Hyundai and Xevo (2018)
- Honda & Connected Travel (2019)
- Visa & SiriusXM Connected Vehicles Service (2019)
- Mastercard & Daimler (2020)

In addition to these SumUp and Mastercard announced a service for Ford Commercial vehicles in November 2020 designed to support small business owners. The service will run in Germany, France, Italy, Spain and the United Kingdom.

Hyundai has also recently launched the Genesis GV80 in Korea with support for in-vehicle payments.

Question 17:

Do you see in-vehicle payments become a use case in the EU "GAIA X" initiative by open innovation through collaboration of best of breed companies in the payment area ?

Yes. This is perfectly possible, but such a decision would, in line with the general GAIA X model, need to company from the collaboration of industry players and member countries.

Other

Question 18:

What is the role of the Telecoms industry to enable in car payments?

Mobile network operators have a very important role to play as they are able to provide additional layers of security across the network. They also ensure the Quality of Service needed; to make sure that the experience is in line with user expectations.

With the deployment of 5G technology and enhanced Radio Access Networks, the core infrastructure and network response times required to support in-vehicle payments are being deployed.

Contact Details

Our panelists have made their contact information available if you'd like to reach out in anyway

Andrew Till
GM of Automotive,
Trustonic

andrew.till@trustonic.com
www.trustonic.com

Frank Leveque
Partner, Vice President Automotive & Transportation, Frost & Sullivan

franck.leveque@frost.com
ww2.frost.com

Frank-Michael Kamm
Product Manager, Digital Solutions/Secure Transactions and Service, Giesecke+Devrient

frank-michael.kamm@gi-de.com
www.gi-de.com

Minh Le
Head of Connected Vehicle & Emerging IoT Offerings, Worldline

van-minh.le@worldline.com
worldline.com
https://www.com/

Column Duffy
Director, Technology Innovation & Strategy, Cyber and Intelligence Solutions, Mastercard

colum.duffy@mastercard.com
www.mastercard.co.uk