TRUSTONIC

A quick guide to R155 and R156 regulations and how TEEs can help you meet them

In recent years, the presence of automation and digitalisation in the automotive industry has positively soared. According to think tank Transforma's 'Connected Car Overview, 2020-2030' report, the connected car space is expected to reach 2.5 billion connections by 2030, following ever-growing calls from consumers for more connected, seamless driving experiences.

The report also goes onto highlight that connected cars are beginning to represent one of the most significant groups of application for Internet of Things [IoT] technology, forecast to contribute 23% to overall IoT spend by 2030, despite having less than an 8% share of all IoT devices. It is, therefore, clear that digital devices are already playing a key role in vehicle evolution and will continue to do so in the future.

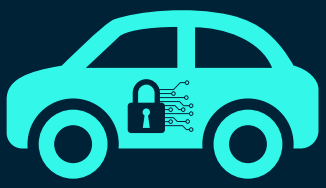
With the rapid growth of automation and digitalisation across the automotive sector comes a heightened focus on cybersecurity. This is because, as more and more digital devices are added to vehicles, the threat of cyberattacks grows exponentially. For example, a recent study revealed that, in 2022, the number of Application Programming Interface [API] related cyberattacks surged by 380%, compared with the previous year. Meanwhile, remote keyless vehicles thefts and break-ins accounted for 18% of total remote incidences, highlighting that the demand for such software-enabled conveniences doesn't come without significant risk to the industry.

To respond to the challenges and vulnerabilities that digitalisation poses to vehicle users, the Global Form for Harmonisation of Vehicle Regulations of the United Nations Economic Commission for Europe [UNECE] published two robust cybersecurity regulations in 2021. These are UNECE R155 Cyber Security and Cyber Security Management System [CSMS], and R156 Software Update and Software Update Management Systems [SUMS]. While R155 and R156 have both been in force for the approval of new vehicle types since July 2022, they are set to be applied to all vehicles produced from July 2024 onwards. While these regulations aim to harmonise vehicle cybersecurity systems across countries and regions around the world, the purposes they play differ somewhat. As such, it is important to establish exactly what R155 and R156 cover.

R155 & R156

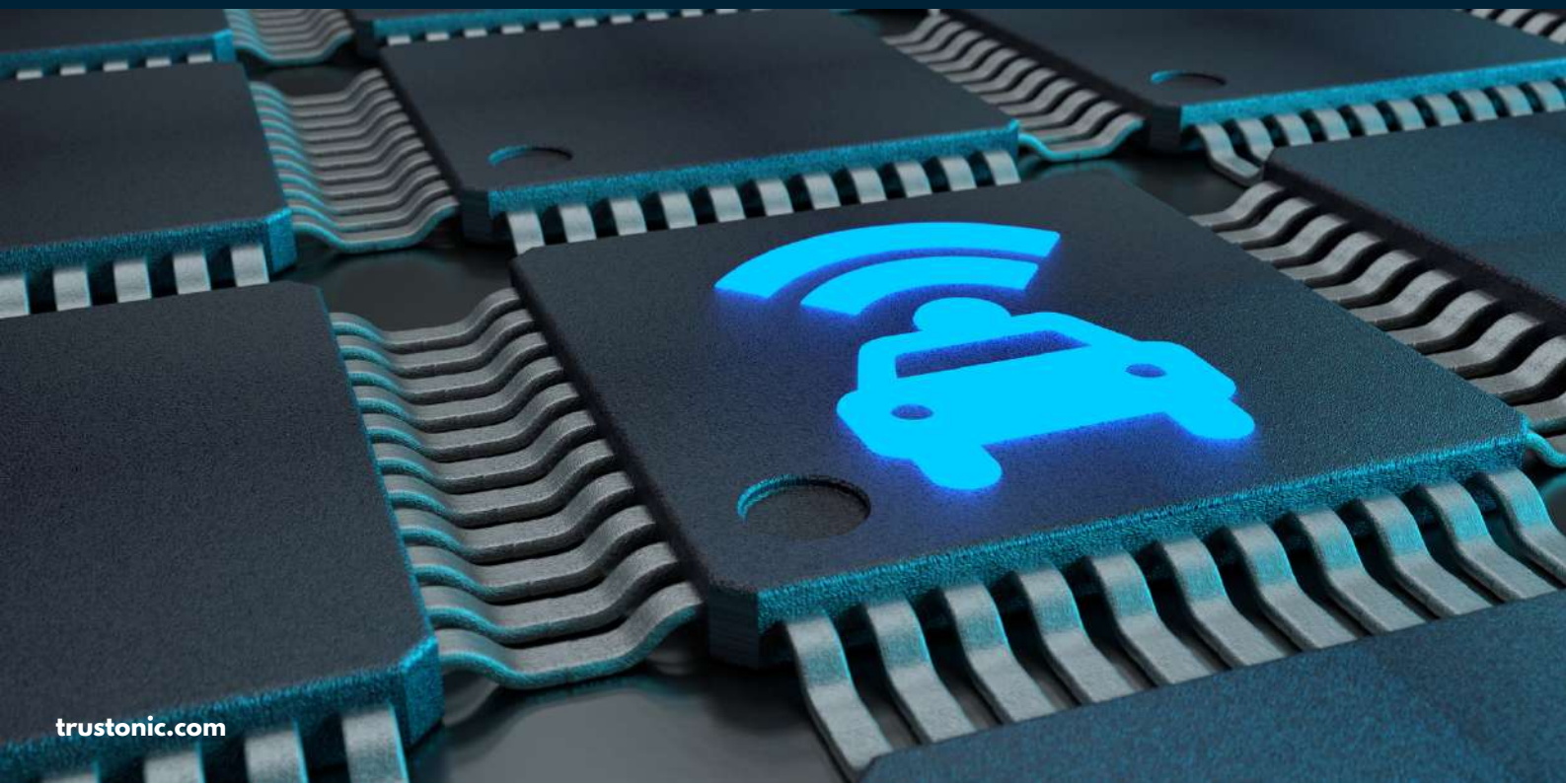
Despite the similarity between their names, R155 and R156 are designed to address different areas of vehicle cybersecurity.

As its full title suggests, R155 is focused around providing uniform provisions for vehicle cybersecurity and cybersecurity management systems. Under the regulation, automotive original equipment manufacturers [OEMs] are required to set up and implement a management system that helps protect the integrity of vehicle cybersecurity. In this sense, R155 is designed to ensure cybersecurity at an organisational level, mandating that cybersecurity principles permeate throughout the business as a whole, as well as its processes. However, it is also centred around the product itself and Type Approvals, and on ensuring the design of the vehicle architecture, risk assessment, and implementation of adequate security controls.



The requirements of R155 are strongly influenced by ISO/SAE 21434, a standard developed by the International Organization for Standardization [ISO] in conjunction with the Society of Automotive Engineers [SAE].

Like R155, ISO/SAE 21434 focuses on the cybersecurity risks associated with the design and development of car electronics, and provides updated guidelines for security management, continued security-related activities, and risk assessment and mitigation methods. As such, it has been pivotal in the creation of processes for R155, and for ensuring Type Approval.

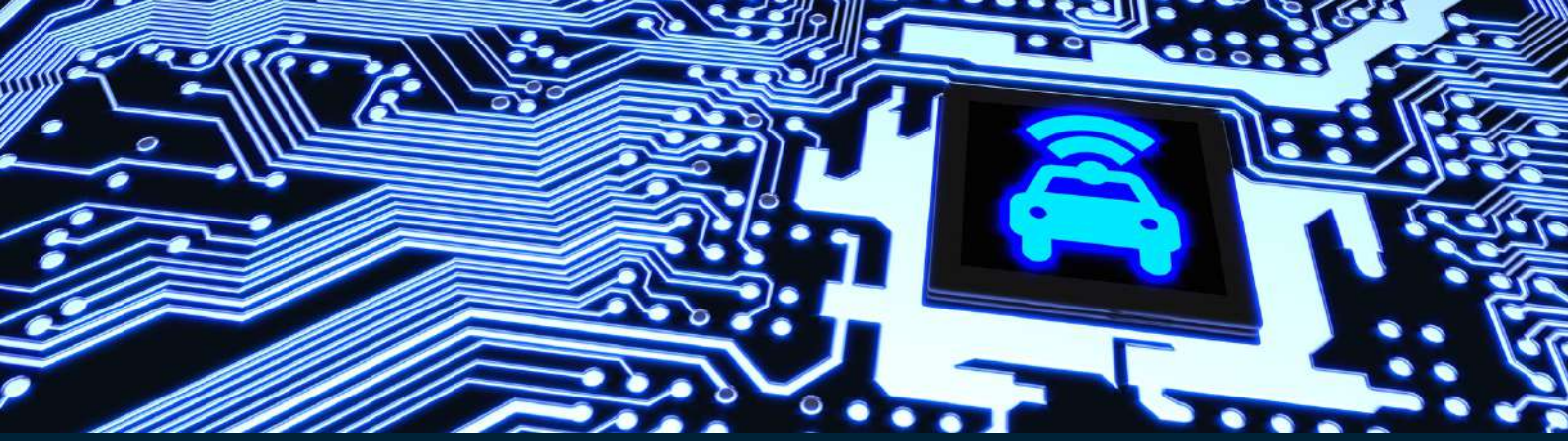


R156, meanwhile, covers uniform provisions for vehicle software updates and software update management systems. It requires OEMs to implement, at an organisational level, a raft of core processes. These include:

- Processes for configuration control for recording the hardware and software versions relevant to a specific vehicle type, including integrity validation data for the software
- Processes for identifying the software and hardware on a vehicle relevant to a specific UN regulation and tracking if that software changes
- Processes for verifying the software on a vehicle component and what should be there
- Processes for identifying interdependences of systems, especially with regards to software updates
- Processes for identifying target vehicles and verifying their compatibility with an update
- Processes to assess if a software update will affect Type Approvals or other legally defined parameters for a given target vehicle
- Processes to assess whether an update will impact the safety or safe driving of a vehicle
- Processes to inform consumers of updates
- Processes to document all of the above, making it available for inspection at an audit
- Processes to ensure the cybersecurity of software updates before they are implemented into a vehicle

In summary, both R155 and R156 require OEMs to take action in four key aspects:

- Managing vehicle cyber risks
- Securing vehicles by design to mitigate risks along the value chain
- Detecting and responding to security incidents across their vehicle fleet
- Providing safe and secure software updates and ensuring vehicle safety is not compromised, creating a legal basis for Over the Air [OTA] updates to on-board vehicle software



Why comply?

Compliance with R155 and R156 is essential for securing Type Approval and, therefore, market access. As such, OEMs must adhere to the regulations to avoid a sales ban in the corresponding areas of application – i.e., the 64 countries where UNECE regulations are in enforcement.

However, gaining Type Approval is not the only reason why OEMs should make sure they are compliant with both R155 and R156. There are a number of other reasons why adherence is so important. For example, failure to fully embrace these mandatory regulations could result in other penalties and fines, which could prove costly for OEMs. With the automotive industry strongly focusing on future digital revenue streams it will also be important that 3rd party content and service provides have confidence in their vehicles. Furthermore, this failure to take cybersecurity seriously enough can badly damage the reputation of the OEM in question. For example, a manufacturer who doesn't treat the cybersecurity of their vehicles as a top priority may choose only to do the bare minimum that's required of them to achieve Type Approval. Clearly, the OEM will have done enough to meet the regulations, but if they then experience a cyberattack and their security architecture isn't robust enough to deal with it, this will be looked on very poorly by consumers. Conversely, an OEM that tries its best not only to meet R155 and R156, but also goes the extra mile to ensure that their security architecture is as strong as possible, will be far more resilient in the event of an attack. This means that customers are far more likely to use their products, especially with consumers becoming increasingly aware of the threats that cyberattacks pose to both vehicle safety and data integrity. While it is true that the convenience that IoT technology provides motorists has largely driven the surge in the use of connected devices within vehicles, many customers recognise the need to balance this convenience with security. Indeed, a Consumer Review conducted by Deloitte found that, with the risk of cyberattacks growing, 84% of consumers now expect organisations to be held responsible for ensuring the security of user data and personal information online. If OEMs want to retain and grow their share of the market, therefore, they can't afford to shirk their responsibility for ensuring vehicle cybersecurity. After all, failing to do so could cause customers to lose faith in their brand, and switch over to competitors who have properly addressed their cybersecurity responsibilities.

The clock's ticking...

It's clear, therefore, that OEMs should not ignore R155 and R156, and that action must be taken. With the date when the regulations will be applicable to all new vehicle types set for July 2024 though, manufacturers may feel that this gives them plenty of time to ensure compliance. As such, they may decide to put their responsibilities off, believing that they can start to think about them closer to the time.

However, such an approach would fail to address a number of key considerations around R155 and R156. For example, both the implementation time and certification process can be lengthy and complex, so manufacturers don't want to find themselves in a state of unpreparedness when the deadline hits. Additionally, OEMs must bear in mind that they need to incorporate their cybersecurity process not only at project level, but also across the entire organisation.

This is part of the push to make security an organisational philosophy rather than a mere activity, permeating every stage of both the design and production processes, and then throughout the entire lifecycle of the vehicle. Everyone in the company should understand and care about the importance of cybersecurity, and be aware of the potential dangers that attacks pose. On top of making security an organisational priority, OEMs must also ensure that all relevant subcontractors that they work with are compliant with R155 and R156.

Another consideration that manufacturers must make is that R155 and R156 differ from conventional regulations because they are audit based. This means OEMs are required to submit their respective management systems for assessment prior to the maturity date. However, auditors may not always be available at the time, leaving manufacturers unable to carry out the necessary audit ahead of the deadline. Given all of this, it is vital for OEMs to take action now, so that they can ensure that they have everything in place and ready for when R155 and R156 come into force for all new vehicle types.

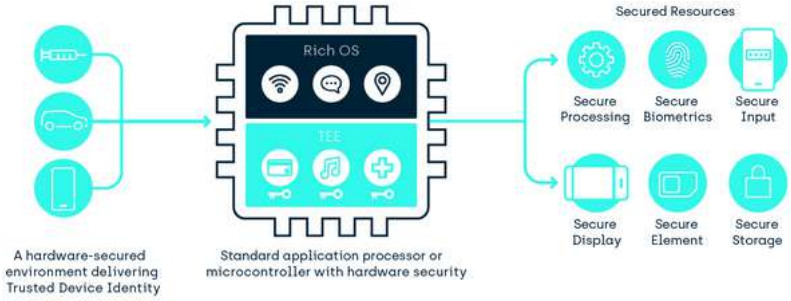
How TEEs fit in

As a leading provider of the industry leading Trusted Execution Environment [TEE], Trustonic has the solution to help OEMs ensure compliance with R155 and R156, and boasts a proven track record of success in working with OEMs to leverage the TEE to enhance the security for FOTA (R156).

Not only does leveraging the TEE ensure that OEMs meet regulations, but that they have the highest possible level of protection. This is because using a TEE that has been certified by technical standards organisation GlobalPlatform is considered best practice for protecting against attacks. Our TEE – which is GlobalPlatform certified – is recognised as best in class, having achieved a Common Criteria EAL5+ rating. This means that the Trustonic TEE has demonstrated the highest possible level of security against both black and white box penetration testing, earning the 'gold standard' for cybersecurity products of its kind. As EAL5+ delivers external, third-party confirmation that our TEE is one of the most mature and secure on the market, the certification helps to further validate our commitment to providing industry-leading security solutions.

The Trustonic TEE is underpinned by operating system, Kinibi, which is a highly mature solution that has been deployed across countless Global Platform based Trusted Applications. The latest iteration, Kinibi 600, provides best-in-class security for automotive environments and boasts updatable libraries for advancing technologies, like crypto, providing the ability to keep the vehicle ever green, while enhancing compliance with the requirements of R156.

The Trustonic TEE has been deployed in more than 25 million vehicles and sits right at the heart of the next generation of secure vehicles. Given that security is a horizontal need across the vehicle, next generation vehicle architecture, leveraging Software Defined Vehicle concepts, must take a 'platform' approach to ensuring that systems are secure. TEEs provide OEMs with the necessary flexibility, delivering isolated storage for secret keys and privacy sensitive data, as well as offering flexible and performant security-critical processing. Unlike hardware solutions, which typically only provide key storage and limited functionality, or pure software solutions, which can be easier to attack, TEEs are a mix of security focused software leveraging isolation features. They represent a highly mature technology, with billions of devices making use of certified TEEs today.



As the deadline for R155 and R156 looms, OEMs who not only want to ensure they are compliant, but also pull ahead of their competitors by demonstrating their extra commitment to cybersecurity, should be implementing the Trustonic TEE now.

Conclusion

Connected devices have become part and parcel of modern life, and the level of convenience and flexibility that they provide are driving their use in vehicles. It is clear, therefore, that the future of vehicle architecture lies in greater connectivity, with those manufacturers who can provide the most seamless connected experiences likely to win favour with motorists.

Despite the clear benefits that connected devices bring, OEMs cannot ignore the considerable risks that they pose to driver privacy and safety – even if consumers do not recognise the threat themselves. The fact of the matter is that, as in-vehicle devices become increasingly sophisticated, so too do the methods that hackers employ to carry out attacks. This is precisely why it is so vital for OEMs to take their responsibilities to cybersecurity seriously. As the threat landscape continues to evolve – and a greater number of complex attacks are committed – cybersecurity must evolve in kind.

OEMs owe it to themselves, their customers, and the wider automotive industry to comply with R155 and R156 and, in doing so, help to build trust in in-vehicle digital technologies.