VDA German Association of the Automotive Industry

Position

European Cybersecurity Certification Scheme for Cloud Services (EUCS)

1. Summary

The German automotive industry faces huge challenges in connection with the European Cybersecurity Certification Scheme for Cloud Services (EUCS) and the NIS 2 Directive expected soon. The latest official draft of the EUCS dates from 2020, but since that time several unofficial versions have been leaked, leading to considerable uncertainty. In particular, the possible introduction of a new certification “assurance level 4” with attendant sovereignty requirements harbors risks for the deployment of cloud solutions from the major US hyperscalers in the German automotive industry.

The OEMs need scalable and competitive cloud infrastructures for important applications such as the development of self-driving vehicles and vehicle connectivity. Any limitation to European options would restrict competition and represent a retrograde step in digitization. If EU Member States were to implement the sovereignty requirements in different ways, the result would be inefficiency and additional costs along the entire value chain.

The automotive industry recommends limiting the sovereignty requirements to sovereign tasks and highlights the need for a unified EU-wide regulation. This is crucial both to competitivity and to free access to high-capacity cloud service providers (CSPs), especially the hyperscalers with global operations.

2. Current context

The last official draft of the European Cybersecurity Certification Scheme for Cloud Services (EUCS) was published by ENISA in December 2020. Since then, various leaked versions of the EUCS have entered the public domain, which have generated considerable uncertainty in the German auto industry. Risks are perceived relating in particular to the potential impacts of the EUCS in conjunction with the new NIS 2 Directive expected in October 2024, which could make EUCS certification mandatory.

Under the current draft bill for transposing the NIS 2 Directive into German legislation (the NIS 2 Implementation and Cybersecurity Strengthening Act, NIS2UmsuCG), automotive companies will be classified either as “essential entities” or as “important entities”; companies in these categories will be subject to different security and reporting obligations and mandatory certification of their cloud infrastructure.

In the latest official version of the EUCS, cloud applications are divided into three separate certification assurance levels, from 1 (“basic”) to 3 (“high”). The publicly leaked later versions of the EUCS suggest that an additional assurance level 4 (“high+”) is to be introduced. Alongside the requirements placed on cybersecurity, this will entail additional sovereignty requirements. Under the proposal, these sovereignty requirements could only be satisfied if access to the data stored in the cloud is prevented by laws passed in non-EU states.

3. Risks

The question of what requirements under the new EUCS certification scheme will now apply to the NIS 2 categories (“important entity” and “essential entity”), harbors an enormous risk for the German automotive sector. If the new EUCS assurance level 4 is to be introduced with the above-mentioned sovereignty requirements for certain areas of application, effectively it will no longer be possible to use cloud solutions from the established hyperscalers (the US systems Microsoft Azure, Amazon AWS and Google Cloud).

As global players, German automotive companies are crucially dependent on a functional market for scalable and competitive cloud infrastructure for their wide-ranging applications, such as the development of self-driving vehicles and vehicle connectivity. Today's highly competitive market would be artificially restricted, which would be hugely detrimental to the range of services offered and represent a retrograde step in digitization.

Furthermore, auto makers need CSPs with a global network of computer centers around the world in order to serve their customers in the regions where the vehicles are used. This global presence is essential for ensuring high availability and performance of the cloud services that are required for modern, connected vehicle services. At present this is not possible without the US hyperscalers, as European alternatives do not meet today's demands.

Another risk lies in the potentially differing implementation of the above-mentioned sovereignty requirements by the EU Member States. If the Member States were to allocate systems to the EUCS levels in different ways, the requirements applicable to the companies' EU-wide activities (development, production, sales and service, financing) and using connected vehicles in different states would vary, and this would result in marked inefficiency and additional costs along the entire automotive value chain, along with massive disadvantages for individual EU countries.

Even if only a small number of individual business areas of the German OEMs are affected by the sovereignty requirements, this would lead to the loss of synergies and thus to increased costs – which would incidentally also be the case for other major European concerns.

4. Recommendations

The automotive industry believes that EUCS requirements for cloud applications should be formulated to ensure the following:

- In the view of the automotive industry, sovereignty requirements should be restricted to cloud applications used for sovereign tasks. The automotive sector should not be included in this category.

- A unified EU-wide regulation is needed. This is of crucial importance, for example, for vehicles that are transported across national borders, and for Europe-wide financial services. The existence of different interpretations of the NIS 2 Directive and differing sovereignty requirements in the EU would distort the balance within Europe, jeopardize the European single market, and severely hamper competitivity between European companies. From a competition perspective (pricing, innovations, etc. – in short, to avoid a monopoly), it is necessary that several high-performance CSPs exist in competition with one another. At present this is possible only by including established, high-performance hyperscalers with global operations.

Contact persons

Dr. Marus Bollig
Managing director
marcus.bollig@vda.de

Martin Lorenz
Manager of Department, Coordination Unit for Security & Data
martin.lorenz@vda.de

Dr. Julian Weber
Senior Consultant
julian.weber@vda.de

The German Association of the Automotive Industry (VDA) consolidates more than 650 manufacturers and suppliers under one roof. The members develop and produce cars and trucks, software, trailers, superstructures, buses, parts and accessories as well as new mobility offers.

We represent the interests of the automotive industry and stand for modern, future-oriented multimodal mobil-ity on the way to climate neutrality. The VDA represents the interests of its members in politics, the media, and social groups. We work for electric mobility, climate-neutral drives, the implementation of climate targets, securing raw materials, digitization and networking as well as German engineering.

We are committed to a competitive business and innovation location. Our industry ensures prosperity in Germany: More than 780,000 people are directly em-ployed in the German automotive industry.

The VDA is the organizer of the largest international mobility platform IAA MOBILITY and of IAA TRANSPOR-TATION, the world‘s most important platform for the future of the commercial vehicle industry.

If you notice any errors, omissions or ambiguities in these recommendations, please contact VDA without delay so that these errors can be rectified.

Publisher

German Association of the Automotive Industry
Behrenstraße 35,10117 Berlin
www.vda.de/en

German Bundestag Lobby Register No.: R001243 EU
Transparency Register No.: 9557 4664 768-90

Copyright

German Association of the Automotive Industry

Reprint, also in extracts, is only permitted,
if the source is stated.

Version

April 2024