

La solution de traitement des passerelles sécurisés des constructeurs

Cyber Security Management

Hella France

infodiagfrance@hella.com

Chiffres clés

Seulement

15

Sont nécessaires pour s'inscrire en tant qu'utilisateur

13

Constructeurs couverts

Plus de

61

Modèles avec sécurisés

Depuis

2020

32,290

Passerelles déverrouillées en 2022

0 €

Aucunes licences supplémentaires requises

Cyber Security Management

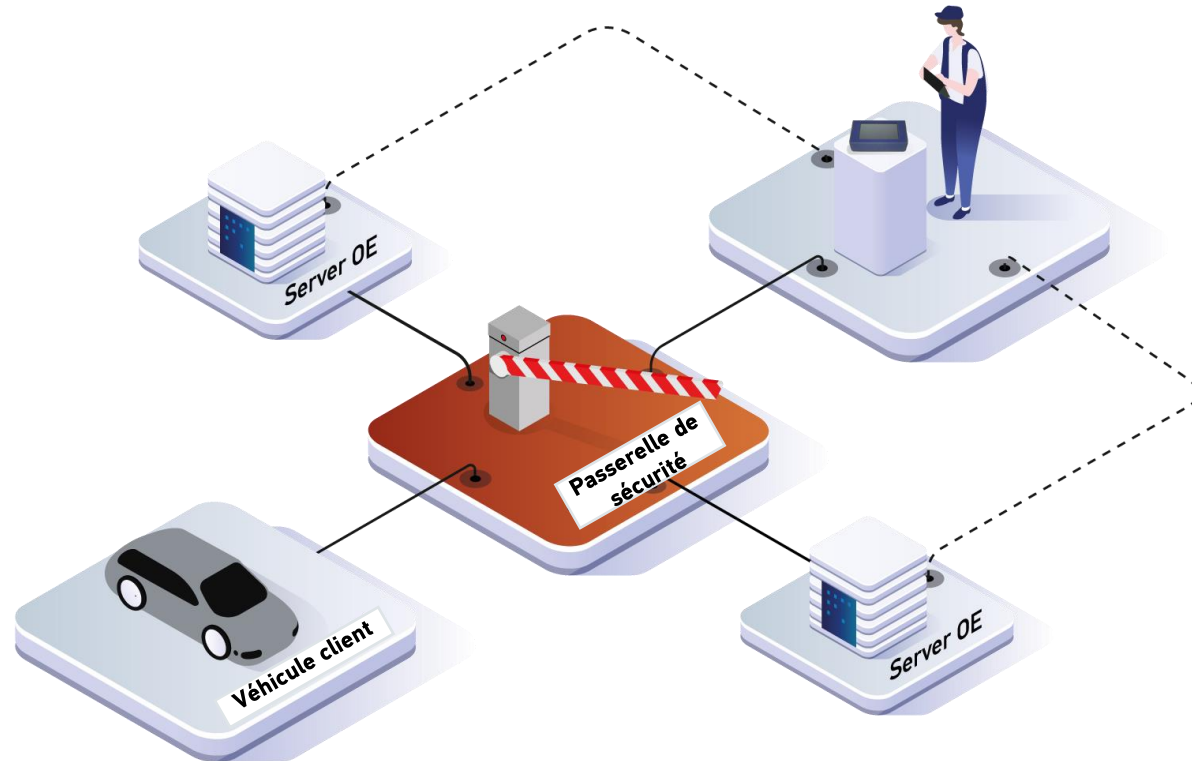
Solutions des constructeurs

Comment déverrouiller les passerelles de sécurité ?

Les garages doivent passer par les portails mis en place par les constructeurs. Souvent le portail « Euro 5 » (Server OE) est indiqué ainsi qu'une interface de communication véhicule répondant à la norme SAE J2534. Chaque constructeur propose une solution technique différente, les coûts associés sont également très différents selon les constructeurs mais ces derniers ne sont pas négligeable. La souscription ainsi que l'utilisation est complexe, chronophage et nécessite une gestion quotidienne complexe.

Chaque constructeur à son système:

- *FCA SGW*
- *Renault Gateway Module*
- *Mercedes CeBAS, Seed&Key*
- *Volkswagen Sfd*
- ...



Cyber Security Management

La solution Hella Gutmann CSM pour les réparateurs indépendants

Une solution simple et identique quelque soit le constructeur !

Multimarque ! La solution CSM est une prise en charge centralisée des accès et authentifications aux différents portails constructeurs.

Une solution pensée pour les ateliers !

La solution CSM permet à tous les employés d'un atelier de s'identifier sur l'outil de diagnostic. Leur identifiant personnel est ensuite valide sur tous les outils de diagnostic Hella Gutmann Solutions

Une solution économique !

Un cout maîtrisé, une solution utilisable immédiatement après inscription.

Une solution rapide !

Pas de délai d'attente entre l'inscription et l'accès aux véhicules.

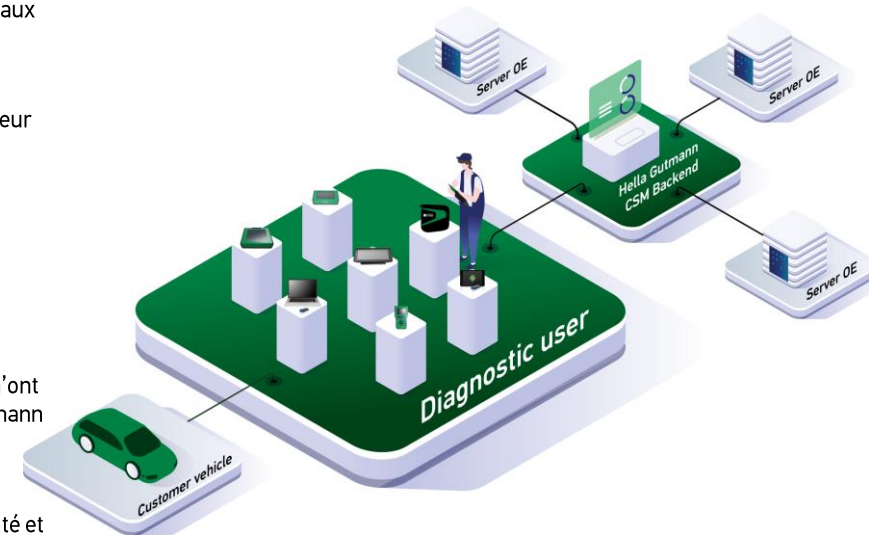
Une solution conforme au RGPD !

La solution garantit une traçabilité et une pseudonimisation des utilisateurs. Les constructeurs n'ont pas accès aux données contrairement à l'enregistrement en direct via les portails Euro. Hella Gutmann Solutions maintient la traçabilité et peut la mettre à disposition des autorités (police, justice).

Une solution d'avenir !

La solution CSM a été conçue pour répondre à toute les solutions futures grâce à ses fonctionnalité et sa gestion d'utilisateur centralisé sur son serveur sécurisé.

L'ajout de nouveaux constructeurs est constant grâce au travail des équipes d'Hella Gutmann.



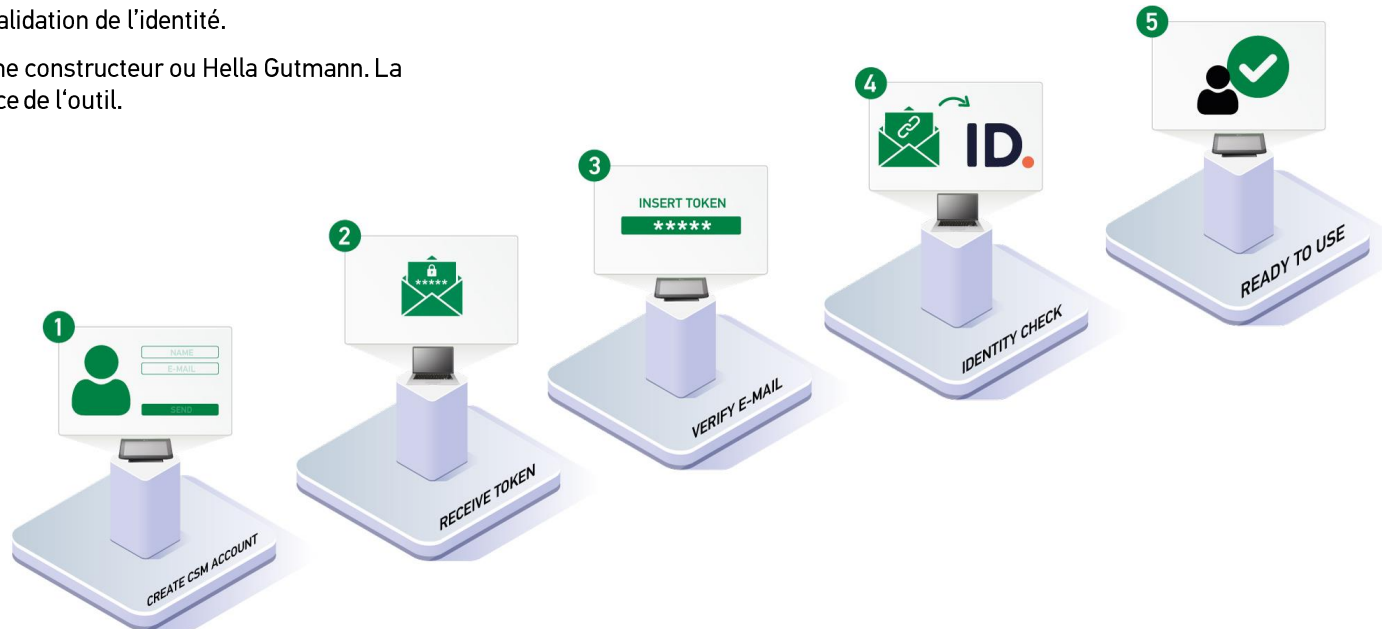
Cyber Security Management

Une inscription simple pour l'utilisateur

Une seule vérification d'identité unique lors du processus de création d'un identifiant personnel.






Accès aux véhicules immédiat après validation de l'identité.

Aucun paiement en ligne sur plateforme constructeur ou Hella Gutmann. La fonctionnalité est incluse dans la licence de l'outil.



Cyber security management

13 brands covered

-  Fiat Chrysler Automotive (Fiat, Alfa Romeo, Jeep, Chrysler)
-  Mercedes-Benz
-  Volkswagen Group (Volkswagen, Audi, Seat, Skoda, Cupra)
-  Kia
-  Renault, Dacia

+ Ford & Porsche traités en « key code ».

Les véhicules concernés ne sont pas équipés de passerelles de sécurité physique. La sécurité est gérée par algorithmes entre l'outil et le véhicule.



Cyber Security Management

Origine et objectifs des systèmes

Au cours des dernières années, les véhicules sont devenus de véritables centres de calculs sur roues. Un véhicule actuel peut comporter près de 150 calculateurs / ECU et environ 100 millions de lignes de code. En comparaison, un avion de ligne en comprend 15 millions, un système d'exploitation de PC grand public 40 millions. Chaque ligne de code présente un risque d'intrusion, autant pour le véhicule lui-même que pour les systèmes auxquels il peut être connecté tels les services de télématiques, la de personnalisation de contenu multimédia ou d'assistance à distance.

Avec la perspective des véhicules autonomes, le nombre d'actuateurs connectés au réseau du véhicule a explosé, tels que les régulateurs adaptatifs, les assistants à la conduite – ADAS –, les systèmes de direction assistée électrique... sont étroitement liés au comportement du véhicule sur la route et donc à la sécurité des occupants et des autres usagers de la route.

De plus, les données produites par les véhicules ainsi que certaines informations personnelles relatives au conducteur doivent également être sécurisées et par définition, accessibles uniquement à des tiers autorisés.

Les risques ont été identifiés très tôt et ces systèmes nécessitent d'être protégés contre toute manipulation ou accès malveillant, en prise directe avec le véhicule ou à distance. L'industrie automobile investit dans le développement et la validation de systèmes anti-intrusion dans tout le cycle de vie du véhicule, autant dans la phase de développement, que la production et également son usage sur route et ses opérations de maintenance en atelier.

Sources:

VDA Verband Der Automobilindustrie, Automotive Security - Position on automotive security, Novembre 2017

McKinsey & Company, Cybersecurity in automotive - Mastering the challenge, Mars 2020

Shiho Kim - Rakesh Shrestha, Automotive Cyber Security - Introduction, Challenges, and Standardization, ISBN 978-981-15-8052-9, Springer 2020

Cyber Security Management

Définition & Applications

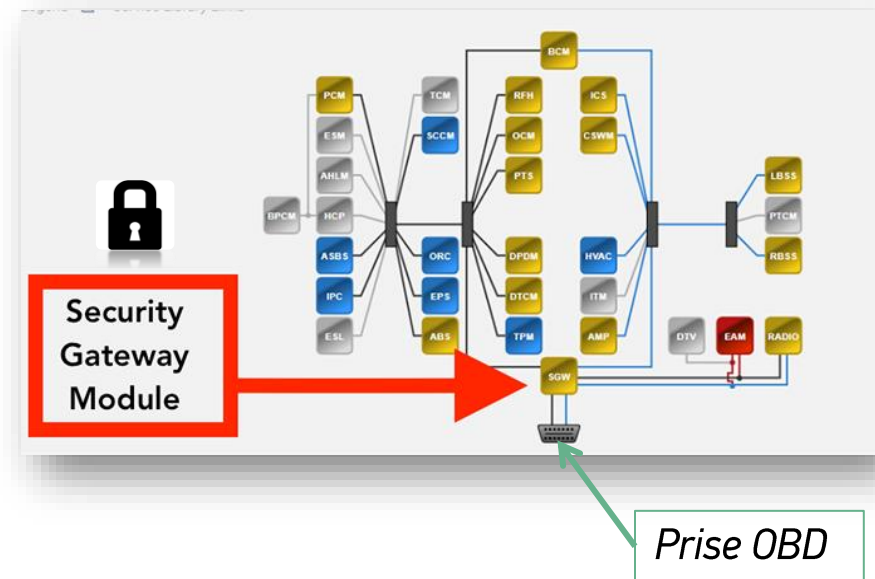
Comment fonctionne une passerelle de sécurité ?

Que ce soit pour une passerelle de sécurité ou pour une authentification, le procédé est souvent le même et est issu du domaine de la cryptographie informatique. C'est une Infrastructure à Clés Publiques ou PKI (*Public Key Infrastructure*). Un certificat est émis par le constructeur, celui-ci est chiffré et signé avec la clé privée appartenant soit au constructeur ou à l'utilisateur. Ce certificat est transmis au véhicule par l'outil de diagnostic. Le calculateur ou la passerelle de sécurité vérifie son intégrité grâce à la clé publique du constructeur enregistrée dans le véhicule. Une fois l'intégrité du certificat validée, l'accès aux calculateurs du véhicule peut-être autorisé.

Le constructeur FCA a été pionnier dans la méthode et établi le nom de Security Gateway Module – SGW.

Quels sont les impacts sur véhicules et les réparateurs ?

Les véhicules ne peuvent plus être réparés et entretenus librement car de nombreuses interventions nécessitent un accès à des fonctions que les constructeurs peuvent avoir sécurisé sur le véhicule. Certaines interventions comme le codage ou la calibration ne sont plus possible, ainsi que certaines réinitialisations d'intervalles de maintenance.



Cyber Security Management



Synthèse

- ✓ Une solution assurant la continuité du diagnostic et de la réparation.
- ✓ Valable pour tous les mega macs en commercialisation.
- ✓ Une utilisation transparente et sûre.
- ✓ Une solution développée pour le futur.
- ✓ Un seul nom d'utilisateur et mot de passe au quotidien.
- ✓ Un cout réduit.
- ✓ Aucune CB.
- ✓ Une inscription unique pour une utilisation multi-constructeurs.