Customer Support Packages

Security Consulting for Automotive

Consulting

Connectivity in cars is revolutionizing modern transport, allowing compelling new services including in-vehicle infotainment, eCall and bCall services and simultaneous connections for a multitude of local devices. It also opens the door to hacking and threats that can jeopardize vehicles, leaving them vulnerable to attacks that can spread worms or malicious viruses compromising car security. To mitigate risk and protect your technology investment, Gemalto is leveraging its unrivaled experience and expertise in digital security for consulting services specifically designed to safeguard vehicles from threats, extending the long life of vehicles and connected car solutions

Description of Services

Our security consulting services begin with an in-depth analysis of your specific situation. A detailed mission report follows providing a thorough account of current strengths, vulnerabilities and threats, as well as recommendations for technology and services to increase security and defend against attacks. Step-by-step deployment instructions offer clients the most cost effective path forward, protecting the most sensitive areas first to remain one step ahead of threats. A final system review provides best practices, conclusions and answers to questions and concerns.

Security Consulting

Design-In
Schematics, Layout Review

HW Tests
Antenna, ESD, Spurious

SW Consulting
ATC, USB, MUX, RIL

Pre-Approval Test
Protocol, Toolkit, SIM (SW,HW)

Production Support
Production line, End of Line

GEMALTO.COM/M2M

gemalto
security to be free

Benefit from proven security expertise

Gemalto is the world leader in digital security and pioneer in M2M technology. More than 1 billion people worldwide use our products and services for telecommunications, financial services, e-government, identity and access management, multimedia content, digital rights management, IT security, mass transit and many other applications.

Gemalto's unique M2M offering includes all the necessary components to simplify and enable the Internet of Things including smart cellular communication modules, secure Machine Identification Modules (MIM)TM, subscription management solutions and an application enablement platform. These solutions and related services serve as a solid foundation for our customers to establish and expand their M2M business and applications with ease and confidence.

The same experts who created and developed these solutions will help to analyze risks and design actions plans to ensure the end-to-end security of your service deployment.

gemalto
security to be free

Consulting methodology

Automotive connectivity services are subject to various types of attacks, such as malicious applications, hacking display mechanism or fraudulent access to services. Through workshops, in-depth interviews, expert analysis and detailed recommendations, Gemalto consultants will help you meet your security goals and implement the best solutions and services at the most optimized cost.

Gemalto has developed a dedicated methodology for automotive implementations, although standard EBIOS methodology can also be proposed upon request.

Outcome of first workshop and income for final analysis

	ASSETS	THREAT AGENTS	SECURITY FUNCTION
ANALYZE OBJECTIVES	Define a list of the main assets that require protection and their attack vectors.	List the main entities that can access the system and possible motivations for attack.	Evaluate the security design in the solution implementation.
EXAMPLES AND MAIN AREAS	Assets: User's financial or personal information, client image, service delivery Attacks paths: JTAG Prob, external access (USD, SD,...) , Network connection...	Car owner, maintenance team, hacker, competitors,...	Supplier audit to validate proper development of customer specifications.

Outcomes of the mission

RISK EVALUATION

OBJECTIVE: Evaluate the impact of security breach for each asset
TYPE OF RISKS: Jeopardize client image, block services, reduce the revenue,
Means to reach it: arbitrary system code execution, steal system data, local malicious code, app isolation bypass...

SECURITY IMPACT & LIKELIHOOD

OBJECTIVE: Provide visibility on client business such as financial or reputation damage on a case-by-case basis.
EXAMPLE: Difficulty to perform the attack, to reproduce the attack on several devices,...

RECOMMENDATIONS

OBJECTIVE: Provide a list of recommendations to increase security to a satisfactory level.
EXAMPLE: Implementation of secure elements, secure boot, additional tests such as penetration

OPTIONAL: PENETRATION TEST

OBJECTIVE: test the actual solution through various attacks and ensure that the implementation reaches base minimum level of security.
ATTACKS EXAMPLES: Port scanning, OS commands, legitimate or illegitimate SMS, USB device mounting, connections through OBD/JTAG,...

gemalto
security to be free

Gemalto Automotive Security

Evaluation and Recommendations

> Evaluation of current solution, assets and threats
> Complete risk analysis
> Action Plan to strengthen security by countermeasures implementation
> Validation Plan

Requirements/Pre-Conditions

> Access to solution design specifications
> Access to development teams and suppliers of the solution
> Dedicated workshop to define the scope and initiate the mission

Results/Outcome

> Detailed report describing the complete methodology, assumptions, risk evaluation and recommendations to provide a consistent level of security.
> Complete validation plan
> Dedicated workshop to explain conclusions

Conclusion and Next Steps

After the delivery of our security experts, the Gemalto consulting team can reinforce the analysis through additional services such as a solution testing phase and accompany your service deployment during its complete life cycle. Trainings, coaching and other consulting services can be further proposed upon request.

Typical comprehensive evaluations take between 1 and 5 months, including regular discussions and workshops.

Gemalto M2M GmbH
Werinherstraße 81
81541 Munich
Germany

GEMALTO.COM/M2M

gemalto
security to be free