Volkswagen: Secure Sharing of Virtual Car Keys App

The Volkswagen Group is one of the world's leading manufacturers of cars and commercial vehicles and the largest vehicle manufacturer in Europe. With ever-increasing amounts of digital and software-based components being used in vehicles, it recognizes the importance of a user experience which is both smooth and secure.

The Challenge – Protecting virtual car key sharing from hackers and malware

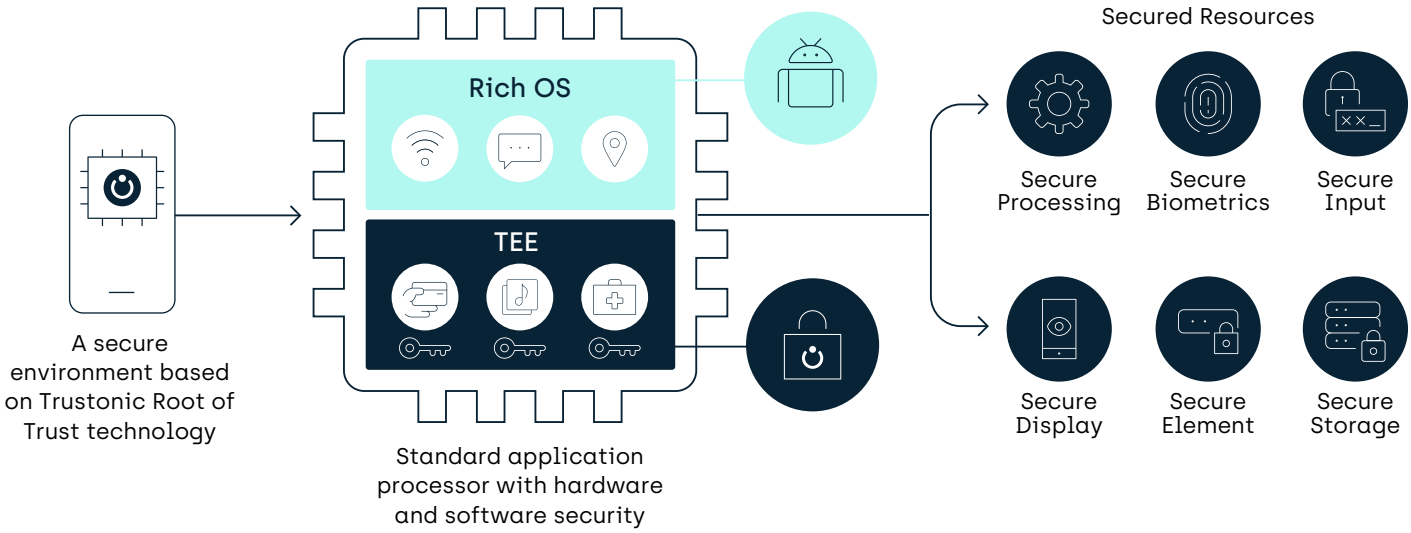
VW recognizes the importance of smart mobility to today's consumers. They are used to managing their lives on their smart devices and virtual car keys are the next step. However, security must be married with accessibility if consumers are to trust in this technology. Importantly, it is about more than just securing the virtual car key on the handset - access rights need to be securely shared across devices when sold, hired, lent or jointly owned. For this reason, it is working to enable its customers to use their smartphones to access their vehicles and to securely share their car keys via a smartphone app. To make this a reality, VW needed to protect its smartphone app from hacking and malware. In addition, to enable the secure transfer of keys, it also needed to ensure that sensitive information and key transfer requests were securely displayed to, and approved by, real users and not some malware simulating a user input.

The Solution – Marrying security with accessibility

VW selected Trustonic Application Security to enable their virtual car keys to be securely shared between smartphones. Working with Trustonic enables VW to benefit from the Trustonic Secured Platform and its Trusted Execution Environment (TEE), with, in the case of VW, the addition of Trusted User Interface (TUI) technology.

The TEE, the hardware-secured operating system (OS), is completely isolated from the device OS (e.g. Android), making it, and trusted applications (TAs) residing in it, well protected from software threats resident on the device. Importantly, Trustonic's is the only 'open' TEE technology that can be accessed by app developers enabling service providers such as VW to deliver experiences that are simpler, richer and faster, because they are more secure.

Trustonic-secured devices protect code in execution, data at rest and in motion, as well as interaction between users and peripherals



The Outcome – sharing virtual car keys in a trusted way

By protecting the virtual key application using Trustonic Application Security, VW can make use of the unique security capabilities contained within modern smartphones. In this case, the application uses the TUI service to securely display information to the user and to ensure that only the authenticated user of the device can confirm the key transfer. Once confirmed, the app uses the secured environment, known as the TEE, to protect user data. The TUI ensures that hackers and malware cannot simulate the user confirmation needed to share a key by mimicking a press on the or by key-logging.

The Benefits

VW now has a solution that brings trust for all stakeholders and opens up new possibilities for its customers. In regards to car ownership, VW can have confidence that only the authorized user can authenticate the transfer of a key and that hackers and malware cannot interfere in this process. Consumers can also have confidence that access to their information and their car are protected on their device.

TRUSTONIC

info@trustonic.com
trustonic.com

200 Cambridge Science Park,
Milton Road, Cambridge, CB4 0GZ. UK

Registered in England with
Company Number 07890730