IDC LINK
Real-time IDC Research® opinion on industry news, trends and events

Hyundai Announces Its Digital Key Mobile App Secured by Trustonic

April 23, 2019

By: Matt Arcaro

IDC's Quick Take

On April 9, 2019, Hyundai and Trustonic, a security software vendor, announced a new Digital Key smartphone application available on the 2020 Hyundai Sonata sedan. Built on a strong virtual and physical security foundation, the solution enables traditional physical car keys to be replaced with a user's smartphone. Hyundai intends to utilize the Digital Key application to support baseline remote vehicle use cases (e.g., remote lock/unlock, remote start, and vehicle tracking), as well as to support emerging use cases for key granting/revocation for mobility-as-a-service (MaaS) car-sharing, automatic car personalization, and third-party access for courier and ecommerce solutions. The Hyundai Digital Key application provides another proof point for consumers wanting to engage with their vehicle digitally through smartphones, smart home devices, and other connected devices.

News Highlights

The Hyundai Digital Key application will be made available along with the release of the 2020 Sonata sedan. This application and overall end-to-end solution leverages the manufacturer's transition to a service-oriented vehicle architecture via vehicle-embedded cellular connectivity and the near ubiquity of smartphone ownership to complement (or completely replace) traditional, physical keys. Hyundai built its Digital Key architecture, using Trustonic's Trusted Application Protection (TAP) platform, to support new and enhanced use case functionality to be delivered by remote over-the-air software update.

Other aspects of the solution to highlight include:

- **Software key protection:** Hyundai implemented a security-first approach to store and protect its Digital Keys. This includes in-vehicle storage of the Digital Keys to ensure unauthorized use or access. Because the automaker has limited control over a vehicle owner's smartphone, the automaker developed its smartphone application using Trustonic's TAP platform. The TAP solution, which is used to secure many other high-trust smartphone applications (e.g., banking and payment), provides Hyundai with a flexible way to build its app to support global privacy and security standards without having to consider compatibility issues and fragmentation. TAP allows the Digital Key app to support the maximum level of security protection available in a given user's smartphone including ideally engaging with the phone's hardware-based trusted execution environment (TEE) or alternatively operating within a software-based TEE.
- **Diverse communication protocol integration:** Hyundai used a multimodal communication approach to ensure sufficient functionality and physical security of its Digital Key solution. This includes integration of near-field communications (NFC) for close proximity (e.g., physical door lock/unlock and vehicle starting); Bluetooth Low Energy (BLE) for intermediate, longer range commands up to 30m (e.g., automatic start); and cellular for longer distance, remote requests. It is worth noting that NFC allows physical access to the vehicle (e.g., door unlock and vehicle starting) even if a smartphone's battery is depleted.

- **Advanced use case support:** Hyundai indicated that its Digital Key solution was designed to support updates for new consumer and business use cases. This includes embracing the concept of car sharing, where the owner can grant/revoke the vehicle's keys to another party. Hyundai also announced its intention to support providing temporary vehicle access for ecommerce and courier use cases including remote fueling and package delivery.

IDC's Point of View

Companion smartphone applications for vehicles have existed for years. These companion apps were initially launched to provide infotainment functionality (e.g., SmartDeviceLink) and greater access to vehicle reporting. However, as manufacturers began to deploy embedded cellular connectivity, the industry added wide area network functionality including support for remote vehicle and telematics services such as remote door unlock/lock, remote start, find my car, and real-time vehicle status reports. These new features have fueled consumer demand for immersive use cases and a more extensive digital relationship with their vehicle.

IDC views the Digital Key mobile application solution developed by Hyundai and secured by Trustonic as an example of an automaker investing to continue diversifying by offering immersive digital services. Hyundai incorporated mobile application security best practices to support a rich feature and capability set available at launch but also to enable a foundation for delivering new and enhanced functionality over time. With Digital Key, Hyundai is embracing the central themes of connected services and the sharing economy to allow its customers the freedom to explore the edges of car ownership including peer-to-peer car sharing.

This announcement reinforces the need for automotive OEMs and suppliers to develop and refine their own digital key strategies and approaches. As such, IDC provides the following guidance to support the development and progress for this strategy initiative:

- **Build upon safety and security.** A vehicle's physical key still represents a principal, primary physical barrier to unauthorized vehicle use. Digitizing this experience for access only (e.g., not driving the vehicle) adds risk mostly to the vehicle owner but utilizing a digital key for all vehicle operations creates the potential for greater risks. Design, test, and validate your digital key solution to ensure the ability to monitor for, detect, and respond to all potential threat vectors.
- **Leverage mobile application security and privacy best practices.** Smartphone applications for digital keys need to operate with the same level of security and privacy as other high-trust applications developed for banking, personal finance, and healthcare. Understand the application requirements in these areas and engage with security vendors developing and delivering these solutions. Pay close attention to a vendor's viability to ensure that the technology will support a typical vehicle life span.
- **Participate in industry organizations and standards bodies.** The security underpinning connected vehicles should not be a competitive differentiator. Instead, the automotive industry, inclusive of manufacturers, suppliers, and regulators, needs to work together to ensure that all vehicle systems and functions are designed, implemented, validated, and supported based on agreed-upon common best practices. Participate in industry organization bodies and forums focused on cybersecurity, as well as digital keys directly, including those as part of the Auto-ISAC, Car Connectivity Consortium (CCC), and IEEE.

- **Design for third-party access.** Although the short-term primary driver for the advancement of digital key functionality is streamlining owner access, the vehicle's extension into ecommerce and the sharing economy must be supported. These emerging areas are increasingly desired for convenience including for package delivery, remote vehicle maintenance, remote fueling, and peer-to-peer car sharing when not in use. Seek out pilots and trials with vendors looking to incorporate vehicle access as part of their service offering to understand specialized requirements.
- **Incorporate redundancies for smartphone inadequacies.** Digital key systems need to consider ways to add resiliency in the case of a smartphone malfunction. The most common malfunction is a battery failure/depletion. In such a case, one remediation approach might be the inclusion of a passive communications alternative channel. But these systems must also be resilient should a smartphone be lost, stolen, or damaged. Tesla's Model 3 keyless systems has built in the redundancy of a credit card–sized RFID keycard to provide vehicle access when an authorized smartphone is unavailable.

Subscriptions Covered:
Next-Generation Automotive Strategies