GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

GlobalPlatform Technology
Virtual Primary Platform

White Paper

February 2022

Document Reference: GPC_WPR_202

Table of Contents

ABOUT US

GlobalPlatform is a technical standards organization that enables the efficient launch and management of innovative, secure-by-design digital services and devices, which deliver end-to-end security, privacy, simplicity and convenience to users. It achieves this by providing standardized technologies and certifications that empower technology and service providers to develop, certify, deploy and manage digital services and devices in line with their business, security, regulatory and data protection needs. Key offerings include secure component specifications; the Device Trust Architecture for accessing secure services within a device; the IoTopia Framework for secure launch and management of connected devices; and the SESIP Methodology for IoT device certification.

GlobalPlatform technologies are used in billions of smart cards, smartphones, wearables and other connected and IoT devices to enable convenient and trusted digital services across market sectors, including healthcare, government and enterprise ID, payments, smart cities, industrial automation, smart home, telecoms, transportation, utilities, and OEMs.

GlobalPlatform standardized technologies and certifications are developed through effective industry-driven collaboration, led by multiple diverse member companies working in partnership with industry and regulatory bodies and other interested parties from around the world.

Learn more about the IoTopia Framework and SESIP Methodology.

globalplatform.org| Twitter | LinkedIn | YouTube | GitHub | WeChat

EXECUTIVE SUMMARY

GlobalPlatform has supported the evolution of Secure Element (SE) technology for more than 20 years. The organization continues to support the evolution of all SE form factors – from distinct hardware elements through to integrated SEs – to support the needs of different use cases and business models in various vertical markets.

As the secure chip ecosystem has evolved, integration has become a notable trend. To support this, GlobalPlatform has defined the Virtual Primary Platform (VPP). The specifications set outlines and standardizes the execution of secure digital services for new SE form factors, like integrated Secure Elements (iSEs) hosted within a System on Chip (SoC). The organization extended these services to other form factors,like embedded Secure Elements (eSEs) in this new specification version.

The specifications support the ability to create a standardized 'virtual'secure area inside a tamper-resistant hardware platform and define the security services that run on this platform, offering a new universal form factor to host and execute secure digital services. At the same time, the specifications maintain the highlevel of security and tamper-resistance achieved by other (previous) SE form factors.

As with these existing SE form factors, VPPs are capable of securely hosting VPP Applications (VPP apps) and their confidential and cryptographic data and are capable of running multiple applications addressing the requirements of different implementations and business needs.

These specifications allow developers to build secure solutions and deploy them across a variety of products. The VPP technology is designed to overcome the dependencies between VPP apps and the underlying platform, meaning that VPP apps can coexist on the same VPP while operating completely independently for issuance, certification, maintenance, and ownership. Thanks to functional and security certification, stakeholders can also be assured that the platform will provide the required secure services.

In December 2021, GlobalPlatform released VPP 2.0. which enhances the level of detail and support for development of VPP solutions for eSE. Version 2.0. is the first integration of VPP with other specifications and comes as a result of GlobalPlatform's ongoing collaboration with standards organization, ETSI. ETSI has already referenced GlobalPlatform's VPP specifications in its Smart Secure Platform (SSP) specifications (ETSI TS 103 666-1, ETSI TS 103 666-2 and ETSI TS 103 666-3) which seek to address IoT, 5G, and other security sensitive sectors.

This white paper introduces the GlobalPlatform VPP specifications to the key stakeholders that will utilize this new way to develop, enable, and manage hardware-backed secure services for new SE form factors. It is GlobalPlatform's aim to extend this work to all SE form factors.

As it has always done, GlobalPlatform continually works to benefit the industry by offering its specifications free of charge, easing the implementation and adoption of new standardized technologies. It thanks its membership for their support and welcomes contributions to its work.

SECTION 1: INTRODUCTION TO VPP

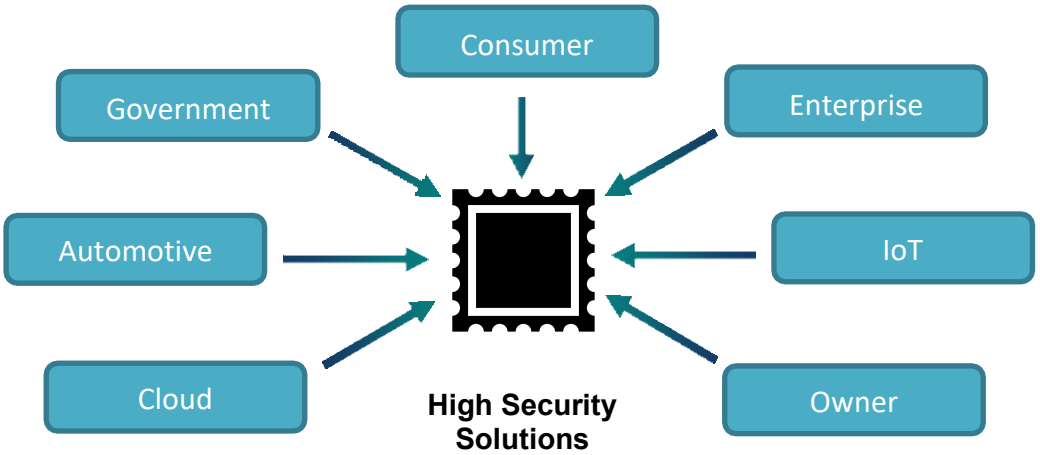
1.1 WHAT IS VPP OFFERING TO THE MARKET?

The wide deployment of SEs across multiple vertical markets is the result of a standardized platform. Existing SEs – such as SIMs, smart cards, smart microSDs, and USB tokens – are stand-alone tamper-resistant hardware platforms, developed as different form factors for different use cases. They are capable of securely hosting multiple applications and their confidential and cryptographic data, addressing the requirements of different business implementations and market needs.

As SE technology evolves there are opportunities to leverage new form factors that support different use cases and business needs and reduce time to market for new solutions. VPP enables this evolution with a set of specifications, initially for iSEs, that maintain the same level of security while providing the flexibility to host and execute secure digital services. It supports a variety of business applications and use cases and gives clear areas of responsibility for the certification process.

The VPP specifications offer chip, device, and firmware makers a standardized way to load and manage firmware – combining the secure high-level operating system (HLOS), its applications, and associated data – in an SE in the device. The SE combines tamper-resistant secure hardware and embedded software to enable security by design and certification of the platform including the BSI-PP0084-2014 (Security IC Platform Protection Profile).

As with existing GlobalPlatform SE technologies, VPP can host and run several separate VPP apps, addressing multiple different use cases – including banking, telecoms, identity, transport, retail, and more – in complete isolation from one another.



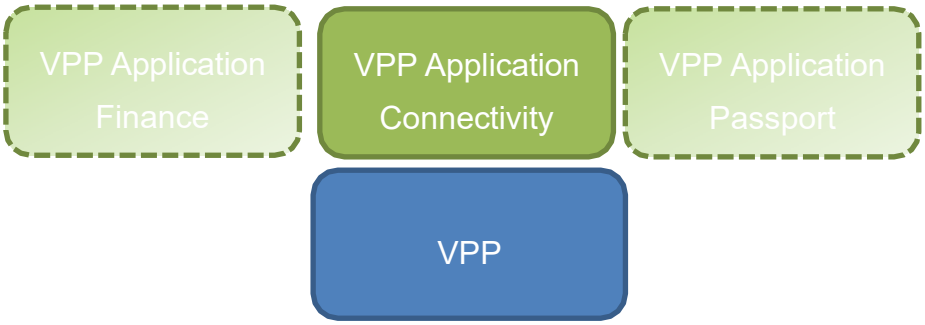
1.2 How does VPP support the evolution of Secure Element technology?

VPP creates a common approach that can be applied across different hardware designs, while offering interoperable secure services for VPP application developers.

Historically, GlobalPlatform focused on managing APIs at the OS level to enable apps to be ported and managed. With this new VPP technology, GlobalPlatform is offering new low-level APIs that abstract the hardware provided by the manufacturer to enable creation of the VPP apps. This allows multiple third parties – such as VPP app providers or service providers – to build services that are based on their own high-level OS and deploy them to the shared hardware platform.

VPP isolates the VPP apps from one another and from the underlying VPP implementation. The technology enables them to independently access the secure services and features offered by the platform, even when multiple exclusive VPP apps are running on the same platform.

Additionally, the VPP specifications standardize the interfaces, the behavior of the APIs, and stakeholders' responsibilities for the tamper-resistant hardware platform. The technology also helps app developers to simplify the porting, testing, and deployment of VPP apps. Importantly, as with all GlobalPlatform secure component technologies, the VPP specifications are independent of the VPP Application use cases.



Developers can port existing execution environments or run native code on top of VPP, offering a straightforward migration path for existing solutions. VPP apps are executed from program code and data, called firmware (in compliance with the VPP Firmware Format specification).

The VPP specifications provide an interface for managing firmware. This interface enables the loading, updating, enabling, disabling, and deleting of firmware. Specific access rights are needed to use the firmware management interface and GlobalPlatform has already standardized the Open Firmware Loader as one way to manage this process.

The VPP specifications define an interface management system that facilitates communication between VPP apps, VPP itself, the other components present within the device, and the outside world.

1.3 WHAT ARE THE BENEFITS OF VPP FOR THE DIFFERENT STAKEHOLDERS?

As with other SE technologies, the VPP specifications bring a range of benefits to several stakeholders. The table below provides a non-exhaustive list of these benefits, mapped against some of the stakeholders that will engage in driving the adoption of the technology.

Table 1: VPP Benefits

Benefit/Stakeholder	Tamper-resistant hardware maker	Device maker	VPP app provider	Service provider
A clearly defined interface between the VPP Application and VPP	✓		✓	
Split of responsibilities clarified	✓	✓	✓	✓
Isolation between VPP apps	✓		✓	
Supports multiple use cases			✓	✓
Ability to port, test, and validate VPP Apps		✓	✓	✓
Ability to accept and certify	✓	✓		✓
Smooth process for launching new solutions		✓	✓	✓
A defined set of capabilities and security features, based on assured level of interoperability that all VPP implementations support		✓	✓	✓
Enables communication with other device components	✓	✓	✓	
Certification according to an established protection profile (PP-0084 or future SoC PP from Eurosmart)	✓	✓	✓	✓
Differentiate by implementing and deploying additional services		✓	✓	✓
Update capabilities of the VPP app			✓	✓
A homogeneously installed base of execution environments across platforms implementing VPP				✓
Reduced effort for maintaining and managing the life cycle of VPP Apps			✓	✓
The IP situation has been clarified thanks to the GlobalPlatform IPR policy	✓	✓	✓	✓

The adoption of VPP technology will be driven by the value that it offers, alongside other SE technologies, to the ecosystem and the key stakeholders.

GlobalPlatform continually works to benefit the industry by offering its specifications free of charge, easing the implementation and adoption of new standardized technologies.

The results of GlobalPlatform's approach and the clear value of these specifications is already being seen. For example, ETSI has already referenced GlobalPlatform's VPP specifications in its Smart Secure Platform (SSP) specifications (ETSI TS 103 666-1, ETSI TS 103 666-2 and ETSI TS 103 666-3) which seek to address IoT, 5G, and other security sensitive sectors.

1.4 How to learn more about VPP

The best way to learn more about VPP is to read through this document and the following specifications, in the order they appear below:

GPC_SPE_140	GlobalPlatform Technology VPP - Network Protocol v2.0
GPC_SPE_141	GlobalPlatform Technology VPP - Network Protocol Extension for the Open Firmware Loader v2.0
GPC_SPE_142	GlobalPlatform Technology VPP - Concepts and Interfaces v2.0
GPC_SPE_143	GlobalPlatform Technology VPP - Firmware Format v2.0

SECTION 2: REVISION HISTORY

Table 2: Revision History

Date	Version	Description
September 2020	1.0	Initial release.
December 2021	2.0	Enhancement of support for eSE and improvements to implementation details for developers.