GLOBALPLATFORM®

THE STANDARD FOR MANAGING APPLICATIONS ON SECURE CHIP TECHNOLOGY

End-to-End Simplified Service Management Framework:

Streamlining Payment Service Management Using GlobalPlatform Technologies

White Paper

January 2016

secretariat@globalplatform.org | www.globalplatform.org |

Table of Contents

About GlobalPlatform

GlobalPlatform defines and develops specifications to facilitate the secure deployment and management of multiple embedded applications on secure chip technology. Its standardized infrastructure empowers Service Providers to develop services once and deploy across different markets, devices and channels. GlobalPlatform's security and privacy parameters enable dynamic combinations of secure and non-secure services from multiple providers on the same device, providing a foundation for market convergence and innovative new cross-sector partnerships.

GlobalPlatform is *the* international industry standard for trusted end-to-end secure deployment and management solutions. The technology's widespread global adoption across finance, mobile/telecom, government, healthcare, retail and transit sectors delivers cost and time-to-market efficiencies to all. GlobalPlatform supports the long-term interoperability and scalability of application deployment and management through its secure chip technology open compliance program.

As a non-profit, member-driven association, GlobalPlatform has cross-market representation from all continents. 120+ members contribute to technical committees and market-led task forces. For more information on GlobalPlatform membership visit www.globalplatform.org.

Publication Acknowledgements

GlobalPlatform wishes to offer special thanks to the members of the Systems Committee and the End-to-End Simplified Framework Working Group, and their respective organizations for their involvement in developing this White Paper.

Contributors include the following:

Members:

German Blanco – MasterCard Business Leader

GlobalPlatform Team Members:

Kevin Gillick – GlobalPlatform Executive Director
Gil Bernabeu – GlobalPlatform Technical Director
Lee'ann Kaufman – iseepr – Managing Director
Alliances Management – Operations Secretariat

Intended Audience

This document is intended for product managers, system architects, and other requirements owners looking for a simple way to implement an end-to-end solution for NFC contactless payment applications for mobile devices and who may be new to GlobalPlatform.

The configurations in the End-to-End Simplified Service Management Framework provide requirements for each involved entity including, but not limited to: Service Providers (SPs), Mobile Network Operators (MNOs), Secure Element (SE) Vendors, Data Preparation (DP) Bureaus, Trusted Service Managers (TSMs), and Mobile Device Manufacturers.

Executive Summary

GlobalPlatform has published many specifications which facilitate the secure, interoperable, and scalable deployment and management of multiple embedded applications on secure chip technology. The breadth of GlobalPlatform Specifications provide a wealth of flexibility, thanks to various several technical options which are offered across the infrastructure. GlobalPlatform structures its approach to specification development around three technical committees (Card, Device, and Systems) which bring forward specifications of value to a number of actors in the value chain, such as, Trusted Service Managers (TSM), and providers of specific technologies including, Secure Elements (SE) and Trusted Execution Environments (TEE).

With the extensive reach of its specifications in mind, GlobalPlatform recognized the need to help businesses new to its technology easily understand which parts of the infrastructure are directly relevant to their area of business, in order to quickly and easily develop a complete solution. As a result, GlobalPlatform established an End-to-End Working Group within the Systems Committee to create a simplified framework for deploying a GlobalPlatform value added service on a Near Field Communication (NFC) mobile device, focusing initially on contactless payments. The result was the End-to-End Simplified Service Management Framework [E2E], also referred to elsewhere in this White Paper as the End-to-End Simplified Framework.

The End-to-End Simplified Framework is a new type of implementation guide published by GlobalPlatform. The framework does not contain new technology, and it does not focus on a single specifications group (such as Card, Device, or Systems). Instead, it enables Service Providers to deploy services faster by starting with a basic template of relevant GlobalPlatform Specifications, drawn from the holistic GlobalPlatform technical infrastructure. The framework aims to ensure Service Providers find the most cost-effective solutions that are quick and easy to deploy while ensuring that both functionality and security are retained. Following the End-to-End Simplified Framework ensures both functionality and security.

The End-to-End Simplified Framework helps Service Providers to focus only on the GlobalPlatform Specifications relevant to their core business activity; by doing so, it also helps them avoid navigating through the numerous specifications which are not. The End-to-End Simplified Framework has narrowed the options for Service Providers by providing self-contained end-to-end solutions, based on specific use cases, called “configurations”. Such configurations provide only the necessary specifications relevant to a specific use case collated from across the entire GlobalPlatform infrastructure.

This White Paper explains how to use the End-to-End Simplified Service Management Framework [E2E] to securely deploy a GlobalPlatform value added service in an NFC device.

SECTION 1: Introduction

The mobile ecosystem has evolved over the last decade. Mobile services have developed well beyond providing simple voice communications to now include services such as mobile payment (both online and in-store), biometric authentication, Mobile ID, enterprise services, and healthcare.

Each service must consider different servers, certificate authorities, hardware components, mobile operating systems, software, communications infrastructure (such as mobile networks and NFC interfaces), and more. Providing secure services within this infrastructure is increasingly important, but it is difficult to provide security assurances in an ecosystem where there are hundreds of combinations of components with their associated dependencies and interactions. Services are heterogeneous and may present completely different requirements from one to another. For instance, deployment of a contactless payment service may not have the same requirements as a health tracker application.

The End-to-End Simplified Service Management Framework [E2E] gathers knowledge from several of GlobalPlatform's specifications. The framework uses a small subset of the GlobalPlatform Specifications and it also takes into account the requirements of other organizations such as EMVCo and the GSMA to ensure full compliance. It enables service providers to deploy services faster and easier by narrowing the required reading down to only the necessary sections of the relevant specifications for their use case. Currently, initial configurations have been developed for NFC-enabled contactless payment. The goal of GlobalPlatform's End-to-End Simplified Framework is to establish a baseline from which additional market-specific configurations can be created to simplify deployment for different ecosystems and stakeholders.

The intent of this White Paper is to provide product managers, system architects, and other requirements owners with an initial introduction and overview of the End-to-End Simplified Framework for consideration or guidance throughout an initial implementation. For technical details and specifications, please refer to the GlobalPlatform End-to-End Simplified Service Management Framework [E2E]. The remainder of this White Paper is as follows:

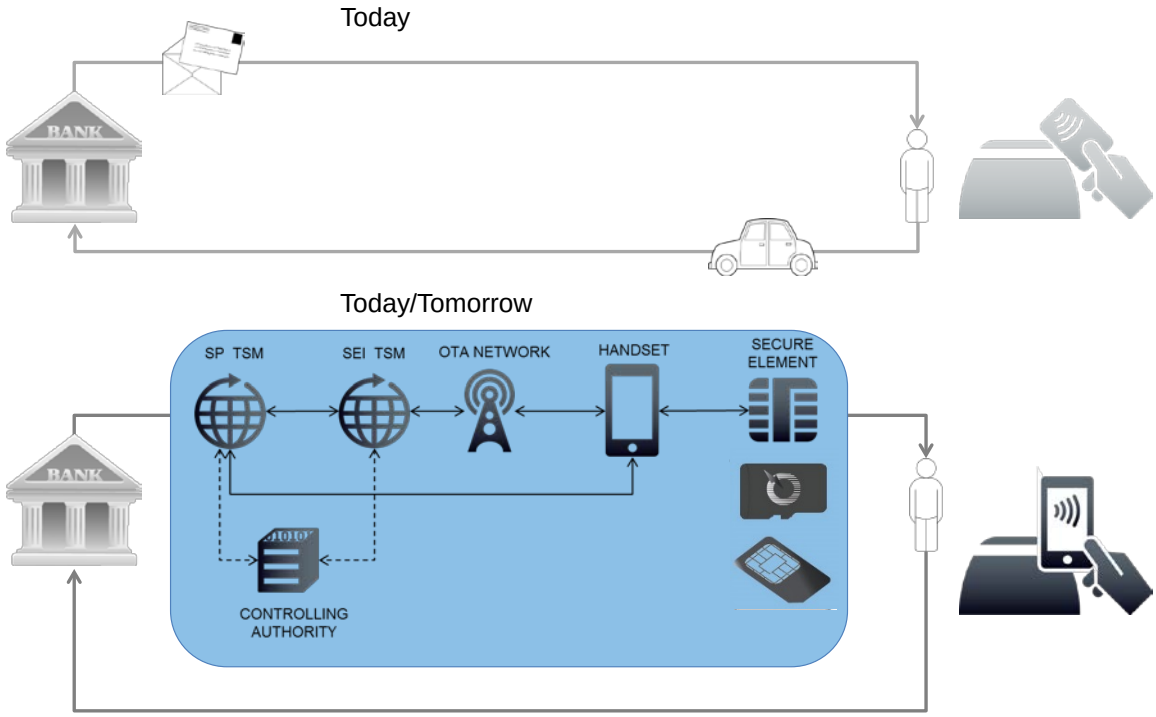
- Section 2 introduces the current ecosystem and describes the benefits of the End-to-End Framework.
- Section 3 outlines the stakeholders and project phases when considering an NFC deployment.
- Section 4 walks through how to use the End-to-End Framework and outlines all of the options provided by the framework.
- Section 5 builds off of Section 4 to provide an example of a UICC Simple Deployment following the End-to-End Simplified Framework.

SECTION 2: Objectives and Value Proposition

Near Field Communication (NFC) technology is long past its experimental phase and is now facing the challenges of scaling and mass-deployment. The development of SE and TSM technologies has resulted in a comprehensive array of technical options to support the implementation of many business models. While flexibility is an important feature in a world where the needs of multiple industries may converge into a single SE, it is important to help Service Providers easily identify the minimum viable feature set required for their own project to aid in the development process, shorten time-to-market, and result in cost-efficiencies. GlobalPlatform is committed to supporting the NFC ecosystem to achieve large-scale deployment through this End-to-End Simplified Framework that provides a comprehensive approach to its specifications.

The End-to-End Simplified Framework has been designed to empower Service Providers to execute mass deployment of NFC services by scaling through the simplicity of the framework. Reducing options is required at all levels to improve and truly facilitate interoperability of technical components. The GlobalPlatform Specifications (and others) provide standard interfacing but they are not prescriptive end-to-end configurations. The delivery of NFC services is a multi-faceted process; current specifications support many different business models and actors, and with so many options available, there is a perceived difficulty in interpreting the technical requirements that may apply to a specific deployment. Provisioning a contactless payment service to a mobile device, as illustrated in Figure 2-1 under Today/Tomorrow, has many more actors and steps to consider when compared to the issuance of a contactless payment card.

Figure 2-1: Delivery of Digital Payment Services



The End-to-End Simplified Service Management Framework provides configurations to fit specific service types. The purpose is to allow Service Providers to simply select the best option from a predefined set of options to match a preferred business model. Service Providers have the flexibility to implement any enhancements to a baseline set up over time to support their specific business needs.

The benefits for service providers span the following areas; reducing costs, reducing time-to-market, standardization, and customization.

Reduces Costs

The End-to-End Framework provides Service Providers with a simple on-boarding process to facilitate the implementation of mobile payment. Even Service Providers who have never completed a GlobalPlatform deployment can follow the steps outlined in the framework to develop their service. The End-to-End Simplified Framework also incorporates the requirements for other industry bodies, such as EMVCo and GSMA, into the implementation guidelines. This reduces time and money spent researching and implementing compliant solutions.

Within the End-to-End Simplified Framework the value of a certain set of options is explained and compared to others. These built-in explanations allow Service Providers to compare a variety of options to find what meets their needs while providing a recommended path to follow, called “configurations”.

Reduces Time

The benefit of providing pre-defined configurations within the End-to-End Simplified Framework is that project definition lead times can be significantly reduced because all considerations usually made during planning have been accounted for within the pre-defined configurations.

Service Providers can save time when liaising with product vendors as the data flow is already incorporated (implemented) in their products if they follow GlobalPlatform Specifications. Easier integration of compliant products increases speed of implementation for a faster time-to-market. Leveraging existing GlobalPlatform standards to ensure portability, interoperability and future expandability.

Standardized

GlobalPlatform provides an open and standardized infrastructure. This means that services can be developed once, even alongside services from other providers, and deployed across multiple platforms to support the desired use case. The GlobalPlatform specifications protect the access and control to services, so there is true and verifiable isolation from other services on the platform to or from other services on the platform.

The End-to-End Simplified Framework provides product vendors with appropriate processes to achieve compliant implementations of the framework. Compliance program tools can then verify; Card, Device, and Systems compliance to GlobalPlatform Specifications. Interoperability is easy when everyone uses the GlobalPlatform infrastructure.

Customizable

The End-to-End Simplified Framework continues GlobalPlatform's commitment to helping Service Providers deliver secure digital services by aiding in completion of each of the project phases to shorten time-to-market. Deployments are customizable now, and in the future, due to the flexible messaging technology within the framework. It is based on GlobalPlatform's open specifications so it is ready and able to be customized to support more sophisticated use cases. There is no limit, but the basic functional steps are outlined and a deployment can be supported without any customization.

SECTION 3: General Architecture and Stakeholders

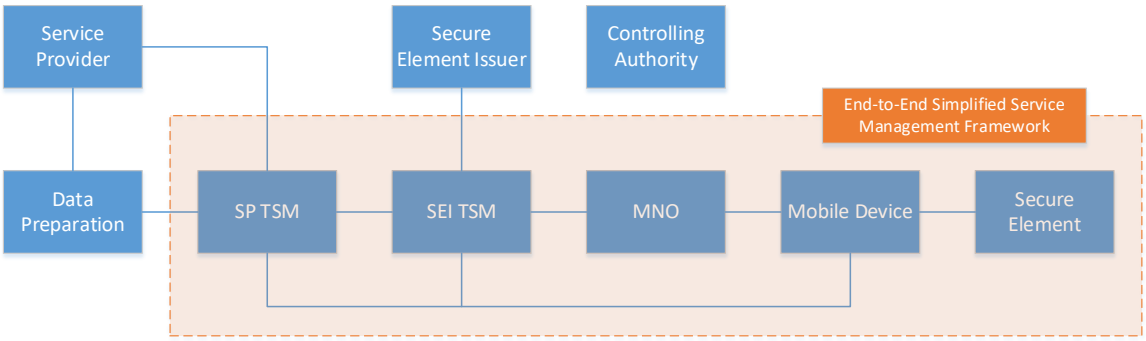
This section gives an overview of all the stakeholders and functional components in the End-to-End Simplified Service Management Framework. The stakeholders described below encompass all the organizations or business units required to originate, distribute or consume a service. Corresponding to each stakeholder, the systems and their components required to deliver the service are described following the major steps of a service in section 3.1.

3.1 *Stakeholders*

There are a number of stakeholders involved in deploying a service and interaction is required between them. Developing business relationships with the correct stakeholders is key to the success of the service. The availability of the End-to-End Framework brings clarity to the industry and encourages standardization and alignment amongst stakeholders and actors.

This section gives a brief overview of the stakeholders and their primary roles and interactions when deploying a new service.

Figure 3-1: Actors in the End-to-End Framework



Service Provider (SP)

A Service Provider is the organization providing the secure service to the end consumer, such as financial services, transportation, or healthcare. For the current scope of this document, the SP is a financial institution that is providing mobile payment services. The SP is required to work with the MNO to deliver applications and services via the MNO's Secure Element.

Secure Element Issuer (SEI)

A Secure Element Issuer is the OEM and provider of Secure Element (Universal Integrated Circuit Card (UICC), embedded Secure Element (eSE), or smart microSD) technologies.

Controlling Authority (CA)

The Controlling Authority is a third party authority that enforces the security policy in a multi-actor environment accessing a Secure Element. It may be used in particular for Secure Domain creation in an SE.

Data Preparation Bureau

The Data Preparation Bureau provides data preparation used to personalize a service. This is outside the scope of the End-to-End Simplified Framework. Each application provider will define its own specification to describe how the data is formatted and prepared.

Service Provider Trusted Service Manager (SP TSM)

The SP TSM is responsible for managing the lifecycle and security of the services and applications being deployed.

Secure Element Issuer Trusted Service Manager (SEI TSM)

The SEI TSM is responsible for managing the end-to-end security of the SE, including the deployment of applications and services. The SEI TSM may be solely responsible for delivering applications, or may authorize a SP-TSM to deploy applications directly without any approvals, or on a case-by-case basis as requests are made to the SEI TSM.

Mobile Network Operator (MNO)

The MNO provides the technical capability to access the mobile environment using an Over-the-Air (OTA) / Over-the-Internet (OTI) communication channel when the SIM is used as an SE.

Mobile Device

The consumer electronics equipment owned by the end customer that interfaces to the MNO infrastructure and contains the SE.

Secure Element (SE)

An SE could be a SIM Card (UICC), smart microSD, or an embedded Secure Element (eSE) that serves as a secure and tamper-resistant storage and execution environment.

The End-to-End framework defines among these actors ‘who’ is responsible for ‘what’ and makes consistent the messaging between all stakeholders.

Knowing which stakeholder to interface with is an important planning aspect of the technical scoping phase. For example, Service Providers establish an SE profile based on the agreement made with the secure element issuer. Service Providers can then define the processes used to deploy applications through the TSM, and determine with the TSM how they will interconnect with other TSMs. The End-to-End Simplified Framework considers all stakeholders within the pre-defined configurations reducing the planning involved in comparison to a traditional technical scoping phase.

3.2 *Project Phases*

One of the biggest challenges faced today by Service Providers is the technical scoping phase of Trusted Service Manager (TSM) infrastructures. It is the first of the four traditional project phases and is usually the longest. Typically Service Providers must build custom products (frameworks) by choosing options from multiple standards (GlobalPlatform and others). This process represents significant effort and requires knowledge of exactly how to assemble all pieces together in a consistent structure.

In order to better explain the value of the End-to-End Simplified Framework, and the points where the framework will provide simplification (of costs and lead times), one must look at the phases of a typical project:

Figure 3-2: Project Phases

Technical Scoping

In a traditional project, it is during the Technical Scoping stage that the SP must acquire a solid end-to-end understanding of the ecosystem. The various roles and responsibilities must be understood in order to fully assess the impact of launching a mobile provisioning project. It is during this stage that the SP will also have to make several technical decisions to define an appropriate architecture. For example:

- What is the consumer experience to subscribe/download a service? Transparent or User Interface driven? Push or Pull Mode? What type of user authentication is to be used?
- What handsets are to be selected?
- What type of Secure Element is required?
- What is the end-user payment experience? Will High Value payments be possible?
- Are there Payment Schemes compliance requirements?
- What is the connectivity and messaging between the SP TSM and the Secure Element Issuer (SEI) TSM? What is the impact on Customer Service?
- What Card Content Management Mode should the SP TSM / SEI TSM implement? Simple, Delegated, or Dual?

Development

In a traditional project, all of the options defined in the technical scoping phase will require development in the form of setup and implementation by all the parties involved (Secure Element Vendors, Application Providers, Data Preparation Bureaus, Trusted Service Managers, Handset Manufacturers, Wallet Providers, Network Operators, Payment Terminal Providers, Payment Schemes, etc.) All components provided by the various actors create outputs from one system that will be used as inputs to another. Therefore consistency across all systems is key in order to ensure that mobile provisioning is well implemented end-to-end. For instance:

- The SP TSM will also need to implement the required connectivity with the SEI TSM. Appropriate messages must be used on both sides e.g. receiving a notification for a stolen handset from one side must be understood by the other as important actions are be triggered (for instance to block the handset remotely).
- Key management procedures must be put in place in order to protect the SE and Issuer keys and to ensure proper usage.

Integration

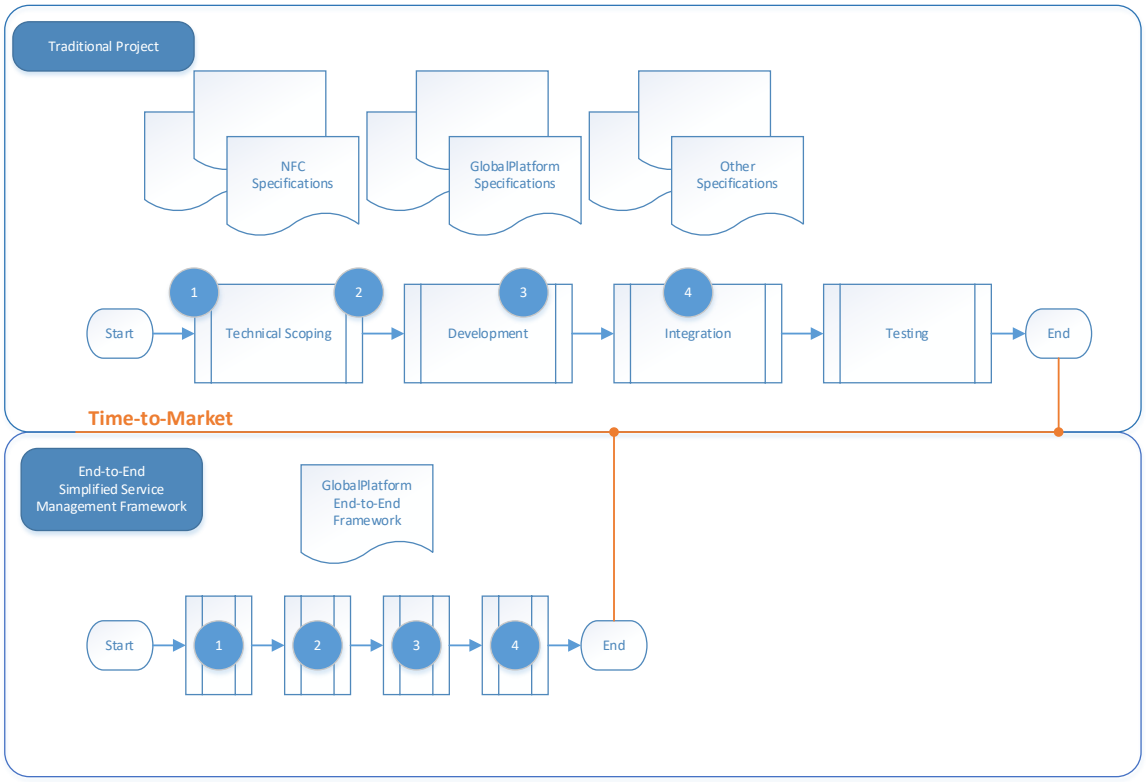
Integration can be costly due to the number of parties involved to deliver a mobile provisioning solution and the large number of options available in the standards for integration. A higher level of interoperability is therefore required in order to reduce these costs. This objective can be achieved by selecting a small set of options and pre-defining configurations for inter TSM integration and, generally speaking, for all components.

Testing

The testing phase tests the interoperability of the implementation. By using a framework to define the earlier phases, the testing phase is simplified by having standard pre-defined configurations that were developed with interoperability in mind.

A traditional project timeline contrast against a timeline using the End-to-End Simplified Framework is shown in Figure 3-3.

Figure 3-3: Project Timeline Comparison



In lieu of the top process of a traditional project, the End-to-End Simplified Service Management Framework provides a set of pre-defined configurations (i.e. standard configurations) that the SP can select off-the-shelf to avoid going through a lengthy technical scoping phase. The selected configuration would then be provided “as-is” to the SP TSM (and to the other involved parties) for development and integration.

With the End-to-End Framework compliant products will be capable of seamless interoperability to reduce integration and testing costs. In order to receive a compliance certificate, appropriate testing is undertaken by Vendors. Furthermore, it is also an objective to create an open market where multiple Vendors can provide several compliant products; and where SPs can select from various Vendors. The reduced timeline using the End-to-End Framework is illustrated in the bottom half of Figure 3-3.

Compared to the traditional project timeline, the time and effort required is reduced for each step when using the End-to-End Simplified Framework. This can equate to a significant reduction in time-to-market. On average, in the world of payment, experience has demonstrated that enabling card portfolio for mobile payments can take 1-1.5 years from project definition through implementation. The primary objective of the End-to-End Framework is to reduce the time and efforts required by Service Providers to define the technical scope of any project. Using the framework from project definition through implementation can reduce time-to-market to as little as six months.

The GlobalPlatform End-to-End Simplified Service Management Framework includes in a single document only the necessary information from all other specifications. Service providers only have to answer a few simple business questions included in the framework in order to start a project. Default pre-defined configurations aid development. Pre-tested components ensure interoperability and make integration and subsequent testing simple and easy.

Regardless of industry, Service Providers aim to deploy services in a way that is fast, simple, and secure. GlobalPlatform supports this goal by requiring only the review of the End-to-End Framework, and the selection and completion of the steps outlined by the desired configuration. Without GlobalPlatform's End-to-End Simplified Framework the research involved in the technical scoping phase and beyond would be extensive, expensive and a diversion of valuable resources and business functions from the core goal of deploying services.

GlobalPlatform's standardized infrastructure ensures that Service Providers do not need to learn the APIs and security architecture of each individual target product. By following the End-to-End Framework Service Providers can develop once and deploy across multiple channels, devices, makes and models in the payment vertical. This portability of service addresses compatibility and scalability issues encountered in many multi-channel and multi-app deployments.

With the End-to-End Framework not only are the major project phases shortened and simplified, so are the milestones within each step, making it easier on everyone involved.

SECTION 4: How to Use the End-to-End Framework

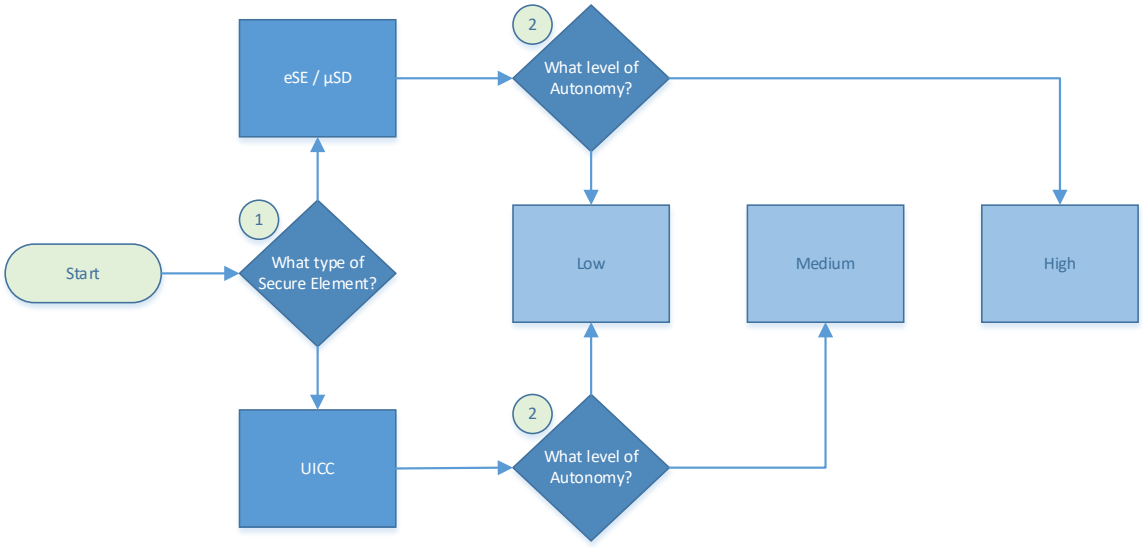
The End-to-End Simplified Service Management Framework [E2E] offers a new way to identify which GlobalPlatform Specifications should be used to deploy a solution in a GlobalPlatform standardized infrastructure. It is not a new specification describing new technology, just a way to piece together existing specifications in a simplified way. The End-to-End Framework is a guide for developing implementations based on GlobalPlatform open specifications.

4.1 *Basic Questions*

GlobalPlatform's End-to-End Simplified Service Management Framework has been developed to enable Service Providers to deploy services within the specific functional and security constraints of their own industry. The framework provides a simple and cost effective way to deploy services by providing a minimalist, fully functional, and secure solution created for a specific service. In the context of GlobalPlatform's End-to-End Simplified Service Management Framework this is referred to as a "Configuration".

The framework provides "configurations" by carefully selecting the options from the specifications that make sense when deploying a specific service in mind. The selection of a configuration starts with a series of basic questions, as illustrated in Figure 4-1.

Figure 4-1: Basic End-to-End Framework Questions



Once these two basic questions are answered, the guide will point the service provider to the appropriate configuration based on their answers. This configuration will outline the exact chapters within the End-to-End Simplified Framework that need to be read by the Service Provider. Using the basic questions to establish the configuration reduces what could be more than 2,000 pages across GlobalPlatform Specifications to around 30 pages within the End-to-End Simplified Framework.

4.2 *Configuration Selection*

Pre-defined configurations are offered by the End-to-End Framework in order to reduce the work for Service Providers. By answering the basic business questions Service Providers will arrive at a configuration that then outlines the specific sections and requirements for a GlobalPlaftorm deployment.

The *End-to-End Simplified Service Management Framework for NFC-enabled Contactless Payment* is the first simplified configuration to be released by GlobalPlatform within the End-to-End Framework. Additional market-specific configurations are forthcoming.

The primary consideration for NFC Payments is the type of SE used: UICC, eSE, or smart microSD. It is expected that a smart microSD will be deployed based on the eSE model. UICCs and eSEs are supported. This is question number one of the configuration selection.

As a secondary consideration the desired level of autonomy for the service can be selected from one of three options: Low, Medium, or High. From these options (illustrated in) comprising question number two, a narrowed selection of configurations are available to choose from, and then any final customization decisions may be decided on and implemented.

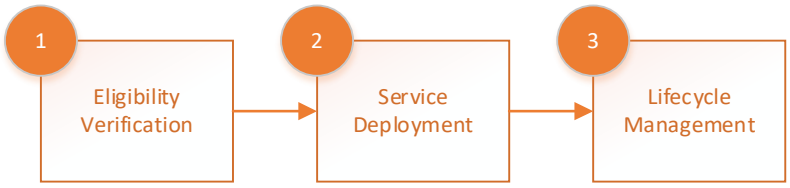
Pre-defined configurations offer a greatly simplified way to get a service project started. In order for the correct configuration to be selected, only two questions need to be answered.

SECTION 5: End-to-End Framework for Payment Service

The End-to-End Framework is developed from a Service Provider perspective, and outlines exactly what is required on the card, device, and system to deploy secure mobile services that align with GlobalPlatform Specifications and configurations. Currently, the End-to-End Framework supports payment services.

While there are the typical project phases, the major steps required of a payment service are Eligibility Verification, Service Deployment, and Lifecycle Management.

Figure 5-1: Major Steps of a Payment Service



Eligibility Verification

Allows the SP to ensure that the End User has the right equipment before attempting remote Service Deployment. With the End-to-End Framework this step is simplified by the pre-defined configurations that SPs have to select from that define the remaining steps in the process.

Service Deployment

Encompasses application loading, installation, personalization, and activation.

Life Cycle Management

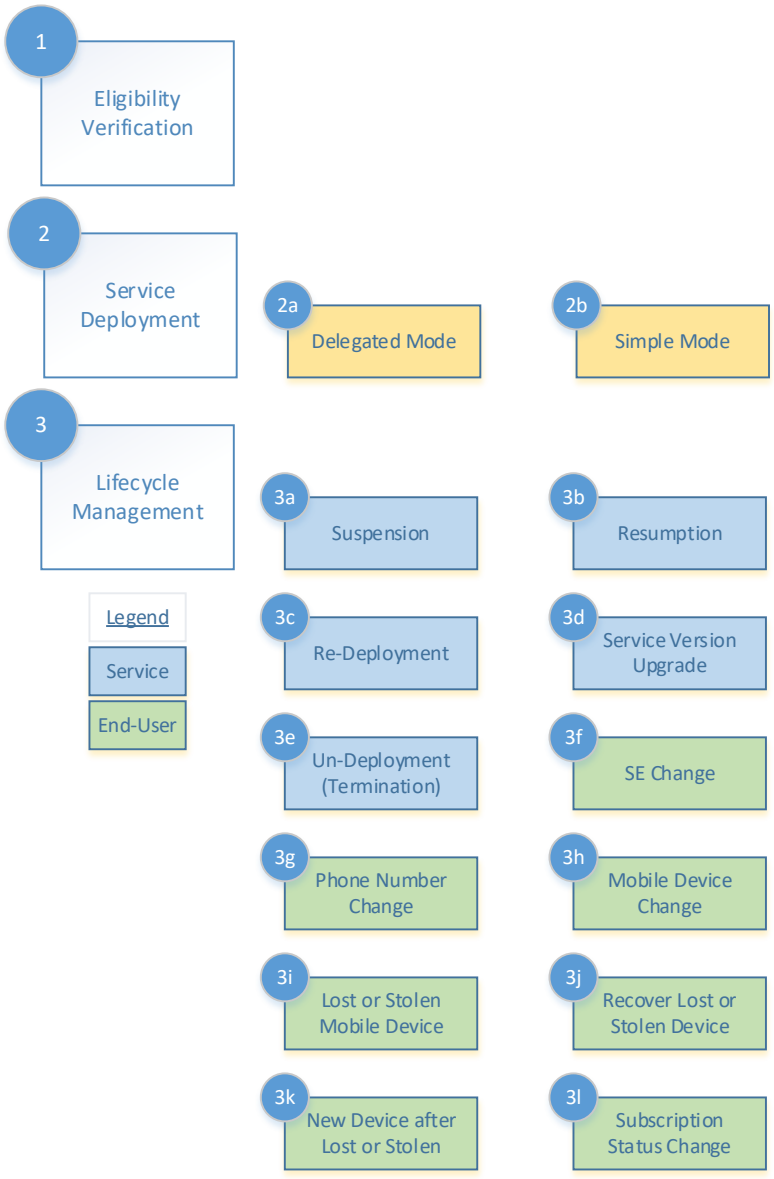
Encompasses management for both the service and end-user.

In the End-to-End Framework the selection of a configuration, as described in Section 4, outlines the necessary considerations to complete the Eligibility Verification step and the SP can move on to the Service Deployment and Lifecycle Management steps quickly and easily.

The Service Deployment and Life Cycle Management of Payment applications are commonly defined independently for each new product or service based on business and technical discussions. In order to streamline the implementation, the End-to-End Framework describes fully functional configurations specific to Payment that will simplify the technical scoping process.

The configuration has a number of other configuration settings and events to consider. Figure 5-2 highlights these considerations for the NFC payment service example.

Figure 5-2: Payment Services Lifecycle Events



After confirming service eligibility, the next step in the process is to deploy the application, which can be done in either Delegated Mode or Simple Mode. For service deployment, a service may be deployed using the OTA channel of either the SP TSM or the SP SEI.

Once the application is deployed, all aspects of the lifecycle must be managed for both the end-user and the service. The Service and End-User Lifecycle events are explained in the following table.

Table 5-1: Lifecycle Events

Event Name	Event	Category	Figure 5-2
Suspension	If the SP or the user determines the service should be suspended, the application will be locked to prevent further use of the service.	Service	3a
Resumption	If the SP or the user determines the service should be resumed, the application will be unlocked to enable further use of the service.	Service	3b
Re-Deployment for Re-Personalization	Allows the SP to change the personalization of the application without re-deploying the application.	Service	3c
Service Version Upgrade	Update the application software and perform re-personalization.	Service	3d
Un-Deployment / Service Termination	Should the service be terminated, the SP will update their back-end and may delete the application or the SP SD.	Service	3e
SE Change	Should the user replace the UICC with a new UICC, the SEI TSM will notify the SP of the change, which will trigger updating account information and re-deploying the application.	End-User	3f
Phone Number Change	Should the end-user change their phone number, this event update all consumer records with the new contact information.	End-User	3g

Event Name	Event	Category	Figure 5-2
Mobile Device Change	Should the user change mobile devices, the application deployment will begin again at eligibility verification and carry through the process to application deployment.	End-User	3h
Lost or Stolen Mobile Device	In the event that a mobile device is lost or stolen, the SP TSM is notified and the account is suspended in a reversible fashion that enables re-enablement at a future point in time.	End-User	3i
Mobile Device Recovery after Lost or Stolen	If a lost or stolen mobile device is recovered, the user notifies the SEI TSM or the SP so that services can be resumed. 1. **New Mobile Device after Lost or Stolen** – if a new mobile device is acquired after the previous one was lost or stolen, the SP is notified that the service should be completely terminated and deployment begins again. 2. **Mobile Subscription Status Change** – should a user's subscription status change through an event the SP is notified, and the SP responds according to their own business rules.	End-User	3j

Each of these lifecycle events are further detailed with the necessary configuration steps and interactions in the End-to-End Simplified Service Management Framework [E2E].

For eligibility verification, service deployment, and the management of lifecycle events, different stakeholders are involved. The End-to-End Framework serves as a central document which outlines the specifications and configurations that are needed for stakeholders in a particular industry to develop solutions to meet their market requirement from start to finish.

SECTION 6: Conclusion

GlobalPlatform's End to End Simplified Service Management Framework [E2E] is ready to help Service Providers deploy NFC services and manage them in the most straight forward and cost effective way.

GlobalPlatform has created technical specifications for more than 15 years. The result is a rich and powerful standardized technical infrastructure that offers several options to cover a variety of use cases. The technology is designed to be service agnostic and ease deployment across devices and platforms.

The simplified End-to-End Framework eliminates the time required for Service Providers to study all the GlobalPlatform Specifications or specifications from other technical standards bodies and, instead, provides a self-contained configuration as an implementation with less overhead compared to a typical project.

The configurations ensure functionality, explain how to perform service deployment and allow Service Providers to manage the life of their application. Development, integration, and testing are greatly simplified thanks to the configurations.

The End-to-End Framework defines each element of the NFC deployment, the connections to each of these elements and to the system as a whole. The framework encompasses the entire solution and shows how GlobalPlatform truly supports the full lifecycle of applications in a simple, secure, and standardized deployment environment.

GlobalPlatform's intent is to expand the configuration options and services which are covered by the End-to-End Simplified Service Management Framework to reflect additional GlobalPlatform Specifications. GlobalPlatform is currently undertaking work to expand the End-to-End Framework to include verticals outside of payment.

All feedback is welcome, and all comments or questions may be submitted to secretariat@globalplatform.org.

APPENDIX A: References

Table A-1: Normative References

Standard / Specification	Description	Ref
GlobalPlatform Card Specification	GlobalPlatform Card Specification v2.2.1, January 2011	[GPCS]
GPCS Amendment A	GlobalPlatform Card, Confidential Card Content Management Card Specification v2.2 – Amendment A v1.0.1	[Amd A]
GPCS Amendment B	GlobalPlatform Card, Remote Application Management over HTTP, Card Specification v2.2 – Amendment B v1.1.2	[Amd B]
GPCS Amendment C	GlobalPlatform Card, Contactless Services Card Specification v2.2 – Amendment C v1.1.1	[Amd C]
GlobalPlatform Device SE Remote Application Management	GlobalPlatform Device, Secure Element Remote Application Management v1.0	[SE RAM]
GlobalPlatform System End-to-End Specification	GlobalPlatform System, End-to-End Simplified Service Management Framework v1.1	[E2E]
ETSI TS 102 622	Smart Cards; UUIC – Contactless Front-end (CLF) Interface; Host Controller Interface (HCI) Release 7	[102 622]

APPENDIX B: Abbreviations

Table B-1: Abbreviations

Abbreviation	Meaning
CLF	Contactless Front End
DP	Data Preparation Bureau
eSE	Embedded SE
MNO	Mobile Network Operator
NFC	Near Field Communication
OS	Operating System
REE	Rich Execution Environment
SD	Security Domain
SE	Secure Element
SEI	Secure Element Issuer
SP	Service Provider
TEE	Trusted Execution Environment
TSM	Trusted Service Manager
UI	User Interface
UICC	Universal Integrated Circuit Card

APPENDIX C: Terminology and Definitions

Table C-1: Terminology and Definitions

Term	Document
Mobile Device	A handheld device: (i.e. a small form factor receiving device suitable for carrying in hand, purse or pocket. The antenna is built-in, either internal or deployable. Normal operation is either at pedestrian speeds walking or at vehicular speeds in a moving vehicle. This is typically the mobile phone or smartphone) or portable device (i.e. A receiving device that uses a built-in or set-top antenna, transportable to different locations. This is typically the tablet.)
Rich Execution Environment (REE)	An environment that is provided and governed by a Rich OS, potentially in conjunction with other supporting operating systems and hypervisors; it is outside of the TEE. This environment and applications running on it are considered un-trusted. Contrast *Trusted Execution Environment*.
Rich OS	An operating system for mobile devices (e.g. Android, Window 8, iOS) that allows the loading of third party applications. The Rich OS runs on top of the Rich Execution Environment.
Secure Channel Protocol (SCP)	A cryptographic protocol referring to a way of transferring data that is resistant to overhearing and tampering.
Secure Element (SE)	A secure component which comprises autonomous, tamper-resistant hardware within which secure applications and their confidential cryptographic data (e.g. key management) are stored and executed. There are three different form factors of SE: Universal Integrated Circuit Card (UICC), embedded SE and Smart microSD. Both the UICC and Smart microSD are removable. Each form factor links to a different business implementation and satisfies a different market need.
Secure Element Access API	An API used by device applications to exchange data with their counterpart applications running in the Secure Element.
Secure Element Application	A software application installed and running on the Secure Element.
Smart microSD	A small, portable, non-volatile memory card format developed by the SD Card Association (SDA).
Trusted Execution Environment (TEE)	The TEE is a secure area of the main processor in a smart phone (or any connected device) that ensures sensitive data is stored, processed and protected in an isolated, trusted environment. The TEE's ability to offer isolated safe execution of authorized security software, known as 'trusted applications', enables it to provide end-to-end security by enforcing protection, confidentiality, integrity and data access rights. The TEE offers a level of protection against software attacks, generated in the Rich OS environment. It assists in the control of access rights and houses sensitive applications, which need to be isolated from the Rich OS. Contrast *Rich Execution Environment*.

Term	Document
Trusted OS	An operating system running in the TEE. It has been designed primarily to enable the TEE using security based design techniques. It provides the GP TEE Internal API to Trusted Applications and a proprietary method to enable the GP TEE Client API software interface from other EE. Contrast Rich OS.
Universal Integrated Circuit Card (UICC)	A Secure Element used in the mobile communications industry, as defined in ETSI TS 102 622 [102 622].

APPENDIX D: Table of Figures

APPENDIX E: Table of Tables