Role & Purpose of Privileges in Global Platform

Mohd Hamid

Syscom Corporation Ltd

Abstract- In this paper, applicability of Privileges on SIM Card during installation of applications is discussed. In addition, small descriptions of privileges, privilege coding in Global Platform 2.2 & Global Platform 2.1 is provided.

Index Terms- Global Platform(GP), Security Domain (SD), Issuer Security Domain (ISD), Supplementary Security Domain (SSD), Data Authentication Pattern (DAP), Cardholder Verification Management (CVM)

I. Introduction

Before moving to the topic in context with GP (Global Platform), first understand "**Privilege**"!!!

So as per normal goggling Privilege means, **A special right, advantage, or immunity granted or available only to a particular person or group.**

Similar to its definition, "**Privileges in GP**" is also the rights / advantage given to applications on Card during installation of application on card. Privileges may be added or revoked during the Life Cycle of an Application. Applications can be:

- Issuer Security Domain
- Supplementary Security Domain
- Normal Application

II. Privilege Definition

Table 1: Represents the different types of privileges, their applicability along with small description

Privilege	**Description**
Security Domain	• A Security Domain (SD) is an application which acts as the on-card representative for an off-card entity (*e.g. the Card Issuer or an Application Provider*). • SD's holds keys & mechanisms which can be used to support operations on cards. • All cards have one mandatory Security Domain i.e. Issuer Security Domain (ISD). • When this privilege is set, application acts as a 'SD' and differs from a 'normal' Application.
DAP Verification	• When application Provider may require that their Application code to be loaded on the card shall be checked for integrity and authenticity. • The DAP Verification privilege of the Application Provider's Security Domain provides this service on behalf of an Application Provider. • When this privilege is set, application is capable of verifying a DAP. • To have 'DAP Verification'- the application must have SD privilege i.e. the application must also be a Security Domain.
Mandated DAP Verification	• When a Controlling Authority may require that all Application code to be loaded onto the card shall be checked for integrity and authenticity. • The Mandated DAP Verification privilege of the Controlling Authority's Security Domain provides this service on behalf of the Controlling Authority. • When this privilege is set, application is capable of and requires the verification of a DAP for all load operations. • To have 'Mandated DAP Verification' - the application must have SD privilege and DAP Verification privilege.
Delegated Management	• 'Delegated Management' allows an Application Provider's SD to perform: 1. Delegated loading 2. Delegated installation and make selectable 3. Delegated extradition 4. Delegated update to the Global Platform Registry

	5. Delegated deletion 6. To manage Card Content with authorization. • The SD that has Token Verification privilege controls such authorization. • Delegated Management is not a mandated feature of a GP Card • When this privilege is set, application is capable of Delegated Card Content Management. • To have 'Delegated Management' - the application must have SD privilege.
Token Verification	• Token Verification allows a Security Domain Provider, typically the Card Issuer, to authorize any Card Content management operation. • A Security Domain with Token Verification privilege requires the knowledge of keys and algorithms used for Tokens. • This privilege does not provide Card Content management capability. • When this privilege is set, application is capable of verifying a token for Delegated Card Content Management.
Receipt Generation	• Receipt generation allows a SD Provider, typically the Card Issuer, to provide a confirmation for the performed card content management. • A Security Domain with Receipt Generation privilege requires the knowledge of keys and algorithms used for Receipts generation. • This privilege does not provide Card Content management capability. • When this privilege set, application is capable of generating a receipt for Delegated Card Content Management.
Authorized Management	• SD with this privilege allows a Security Domain provider to perform Card Content management without authorization (*i.e. without a token*) • This is valid where the off-card entity is authenticated as the owner (Security Domain Provider) of the Security Domain. • In this case the Security Domain that has Token Verification privilege is not involved. • When this privilege is set, application is capable of Card Content Management • To have 'Authorized Management' - the application must have SD privilege.
Card Lock	• CARD LOCK is present to provide the capability to disable the selection of SD and Applications. • On receipt of a request to lock the card, the OPEN shall check that the current card Life Cycle State is SECURED. • Once the card Life Cycle State is CARD_LOCKED, all applications except the Application with the Final Application privilege shall be disabled. • The card Life Cycle state transition from SECURED to CARD_LOCKED is reversible. • When this privilege is set, application is capable to lock the card.
Card Terminate	• The state TERMINATED signals the end of the card Life Cycle and the card. • In the card Life Cycle State TERMINATED, all communication to the card is directed to the application with the Final Application privilege. • If the ISD is the application with this privilege all commands other than the "GET DATA" command processed by the ISD shall be disabled. • When this privilege is set, application is capable to terminate the card.
Card Reset	• This privilege was previously known as "Default Selected" in GP2.1 • When this privilege is set, application is capable to modify historical bytes on one or more card interfaces. • Few more key points described below under "Privilege Assignment"
Final Application	• Final Application (*when this privilege is set*) is the only Application accessible in card Life Cycle State CARD_LOCKED and TERMINATED. • In the card Life Cycle State TERMINATED, all communication to the card is directed to the application with the Final Application privilege. • If the ISD is the application with this privilege all commands except the "GET DATA"

	command processed by the ISD shall be disabled.
CVM Management	• CVM is a method to ensure that the person presenting the card is the person to whom the card was issued • When this privilege is set, application is capable to manage a shared CVM of a CVM Application. • CVM services (*Retrieving CVM state, setting new value of cvm, verifying cvm*) shall be provided by a CVM Application to other on-card Applications
Trusted Path	• Application (*when this privilege is set*) acts as a Trusted Path for inter application communication. • The objective is that the GP Trusted Framework forwards the unwrapped command to the "Target Application" indicated by the "Receiving Entity". • Flow of APDU Command 1. An APDU command is received by the Application's SD (*Receiving Entity*) 2. Application SD can be the ISD or a SSD. 3. Command is unwrapped by the SD before being passed on to the Global Platform Trusted Framework.
Global Delete	• Global Delete privilege provides the capability to remove any Executable Load File or Application from the card even if the Executable Load File or Application does not belong to this Security Domain. • A Security Domain without Global Delete privilege and with Card Content management capability can only delete Executable Load Files or Applications directly or indirectly associated with it.
Global Lock	• Global Lock privilege provides the right to initiate the locking and unlocking of any application on the card • Works independent of its Security Domain association and hierarchy. • It also provides the capability to restrict the Card Content Management functionality of OPEN.
Global Registry	• Application (*when this privilege is set*) may access any entry in the Global Platform Registry. • The status of an Application (or a SD): its Life Cycle State, Privileges and other parameters registered in the GP Registry, may be accessed by suitably authorized entities.
Global Service	• Application (*when this privilege is set*) provides services to other Applications on the card. • One or more Global Services Applications may be present on the card to provide services to other Applications on the card. • This is the privilege which separates "Global Services Applications" from other Applications.

III. PRIVILEGE ASSIGNMENT

Below described are the important points to be considered while setting privileges.

- Common key points regarding "Card Reset & Final Application Privileges":

1. Only one Application or Security Domain in the card may be set with the "Card Reset & Final Application Privileges" at a time (*e.g. the ISD, a current legacy Application or an Application that requires specific behavior with regards to logical channels*)

2. Once the "Card Reset & Final Application Privileges" has been assigned to an Application, the privilege can be reassigned to a new Application either by deleting the Application which has the privilege, or by revoking its privilege

3. The "Card Reset & Final Application Privileges" is by default assigned to the Issuer Security Domain. It may be reassigned only if the Issuer Security Domain has the "Card Reset & Final Application Privileges" accordingly

4. If the application with the "Card Reset & Final Application Privileges" is deleted, the privilege is reassigned to the Issuer Security Domain

IV. Backward Compatibility

For backward compatibility, where a card supports only privileges 0-7 i.e. Cards with GP 2.1, the following assumptions (**by Global Platform**) shall apply for the remaining privileges.

Table 2: Coding of the remaining privileges

Privilege	ISD	SSD	Other Application
Trusted Path	Yes	Yes	No
Authorized Management	Yes	No	No
Token Verification	Yes	No	No
Global Delete	Yes	No	No
Global Lock	Yes	No	No
Global Registry	Yes	No	No
Final Application	Yes	No	No
Global Service	No	No	No
Receipt Generation	yes	No	No

V. Privileges Coding

Figure 1: Byte 1 - Available for both GP 2.1 & GP 2.2 and follow same coding

b8	b7	b6	b5	b4	b3	b2	b1	Meaning	Privilege Number
1	-	-	-	-	-	-	-	Security Domain	0
1	1	-	-	-	-	-	0	DAP Verification	1
1	-	1	-	-	-	-	-	Delegated Management	2
-	-	-	1	-	-	-	-	Card Lock	3
-	-	-	-	1	-	-	-	Card Terminate	4
-	-	-	-	-	1	-	-	Card Reset	5
-	-	-	-	-	-	1	-	CVM Management	6
1	1	-	-	-	-	-	1	Mandated DAP Verification	7

Figure 2: Byte 2 - Only available in GP 2.2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning	Privilege Number
1	-	-	-	-	-	-	-	Trusted Path	8
-	1	-	-	-	-	-	-	Authorized Management	9
-	-	1	-	-	-	-	-	Token Management	10
-	-	-	1	-	-	-	-	Global Delete	11
-	-	-	-	1	-	-	-	Global Lock	12
-	-	-	-	-	1	-	-	Global Registry	13
-	-	-	-	-	-	1	-	Final Application	14
-	-	-	-	-	-	-	1	Global Service	15

Figure 3: Byte 3 - Only available in GP 2.2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning	Privilege Number
1	-	-	-	-	-	-	-	Receipt Generation	16
-	X	X	X	X	X	X	X	RFU	-

VI. Conclusion

- In card Life Cycle State, the Issuer Security Domain shall initially have the following set of privileges clearly identifying its functionality: Security Domain, Authorized Management, Global Registry, Global Lock, Global Delete, Token Verification, Card Lock, Card Terminate, Trusted Path, CVM Management, Card Reset, Final Application and Receipt Generation.
- Authorized Management and Delegated Management privileges are mutually exclusive
- Other privileges are not mutually exclusive; therefore, one or more privileges may be marked as set for an Application.

VII. Acknowledgement

I would like to acknowledge my co-workers for supporting and encouraging me throughout the course work.

References

[1] GPCardSpec_v2.2, [2] Card_Spec_v2.1_v0601

Authors

First Author – Mohd Hamid, Qualification /Experience: B.Tech .Currently working with Syscom Corporation Ltd, a leading telecom company dealing in SIM and SMART cards. Experience is ~ 9 Years., Email Address: mhamid1984@gmail.com