The response to the last INSTALL [for load, install and make selectable] command completes the combined load, install and make selectable process.

### 9.3.5 Card Content Loading Process

The phases in Figure 9-1 use a combination of multiple occurrences of two different APDU commands (INSTALL and LOAD). The following sequence of APDU commands apply to the loading:

- An INSTALL [for load] command serves as the load request for loading. The INSTALL [for load] command data field details the requirements regarding a Load File;
- Multiple LOAD commands are then used to transport the Load File in blocks according to the size of the file and the communications buffer size of the card;
- Each INSTALL or LOAD command is processed by the receiving Security Domain before forwarding the load request and Load File to the OPEN for processing.

The following runtime behavior requirements apply during the content loading process.

**Load Request Runtime Behavior**

On receipt of an INSTALL [for load] command, the Security Domain performing the load shall:

- Apply its own secure communication policy;
- Apply its own security policy, e.g. check that its Life Cycle State is PERSONALIZED (only applicable to a Security Domain other than the Issuer Security Domain);
- If a Load File Data Block Hash is present in the INSTALL [for load] command, request the OPEN to initiate the hash verification of the subsequent Load File Data Block;
- If the Security Domain performing the load has Delegated Management privilege, check that a Load Token is present in the INSTALL [for load] command;
- If the Security Domain performing the load has the Authorized Management privilege and the off-card entity at the origin of the load request is not authenticated as its Security Domain Provider (see section 10.4 - *Entity Authentication*), check that a Load Token is present in the INSTALL [for load] command;
- If a Token is present in the INSTALL [for load] command, request the OPEN to obtain verification of the Load Token;
- If the Application Provider identifier is present in the load request, request the OPEN to save this in the GlobalPlatform Registry for the Executable Load File.

On receipt of a load request (arising from an INSTALL [for load] command), the OPEN shall:

- Check that the card Life Cycle State is not CARD LOCKED or TERMINATED;
- Check that OPEN and the requesting on-card entity have no restriction for load;
- Check that the requesting on-card entity is a Security Domain with Delegated Management or Authorized Management privilege;
- Check that the AID of the Load File is not already present in the GlobalPlatform Registry as an Executable Load File or Application;
- If an associated Security Domain AID is present and is not the Security Domain performing the load, check that this AID exists within the GlobalPlatform Registry and is registered with the Security Domain privilege. As this equates to the extradition of the Load File, check that the associated Security Domain accepts this extradition. If the associated Security Domain has the

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0101

Ciphered Load File Data Block Privilege, the OPEN shall check that the Load File Data Block is sent ciphered (i.e. with the tag 'D4'). If no associated Security Domain AID is indicated, the Security Domain performing the load is by default the associated Security Domain;

- At the request of the Security Domain performing the load, request the Security Domain with Token Verification privilege to authorize the load request (e.g. to verify the Load Token).

At the request of OPEN, the associated Security Domain shall:

- Apply the Security Domain Provider's policy to accept or reject this load;
- Apply its own security policy, e.g. check that its Life Cycle State is PERSONALIZED (only applicable to a Security Domain other than the Issuer Security Domain).

At the request of OPEN, a Security Domain with Token Verification privilege shall:

- Verify the Load Token.

At the request of OPEN, a Security Domain accepting an implicit extradition shall:

- Apply the Security Domain Provider's policy to accept or reject this implicit extradition;
- Apply its own security policy, e.g. check that its Life Cycle State is PERSONALIZED (only applicable to a Security Domain other than the Issuer Security Domain);

**Load Phase Runtime Behavior**

On receipt of the LOAD commands, the Security Domain performing the load shall:

- Apply its own secure communication policy;
- Discover whether any Security Domain has the Mandated DAP Verification privilege and if so:
  - Ensure that the required authentication data (DAP Block identifying the above Security Domain) is present in the Load File
- Check if the associated Security Domain has the DAP Verification privilege and if so:
  - Ensure that the required authentication data (DAP Block identifying the associated Security Domain) is present in the Load File;
- If authentication data (one or more DAP Blocks) is present in the Load File:
  - Ensure that a Load File Data Block Hash was received during the load request process;
  - Extract the authentication data (one or more DAP Blocks) from the Load File;
  - For each DAP Block of the Load File, request the OPEN to obtain verification of the DAP by the Security Domain indicated in the DAP Block.

On receipt of the Load File the OPEN shall:

- Verify the resource requirements of the Load File (see section 9.7 - *Memory Resource Management*) and that sufficient card resources are available;
- Check that each DAP verification request from the Security Domain performing the load relates to a Security Domain present in the GlobalPlatform Registry with DAP or Mandated DAP Verification privilege and if so request the Security Domain to verify the DAP;
- Compute the hash of the Load File Data Block when verification of a DAP Block or Load Token is requested.

At the request of OPEN, the Security Domain(s) verifying the DAP(s) shall:

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0102

- Verify that the DAP matches with the Load File Data Block Hash received in the load request.

**Load Completion Runtime Behavior**

On receipt of the last LOAD command, the Security Domain performing the load shall:

- Apply its own secure communication policy;
- Request the OPEN to obtain a Load Receipt.

On completion of the load process the OPEN shall:

- At the request of the Security Domain performing the load, verify the Load File Data Block Hash received in the load request;
- Check in the GlobalPlatform Registry if any Security Domain has the Mandated DAP Verification privilege and if so:
  - Ensure that the above Security Domain has successfully verified a DAP;
- Check in the GlobalPlatform Registry if the associated Security Domain has the DAP Verification privilege and if so:
  - Ensure that the associated Security Domain has successfully verified a DAP;
- If one or more DAP verifications were performed, verify the Load File Data Block Hash received in the load request;
- If the Security Domain performing the load has Delegated Management privilege, ensure that the Security Domain with Token Verification privilege has successfully verified a Token;
- If a Load Token was verified, verify the Load File Data Block Hash received in the load request;
- Create an Executable Load File using the Load File Data Block;
- Create an entry in the GlobalPlatform Registry for the Executable Load File indicating its associated Security Domain;
- Create an entry for each Executable Module within the Executable Load File in the GlobalPlatform Registry. This shall include the Application Provider identifier if requested by the Security Domain in the load request. The associated Security Domain for each Executable Module shall be the same as the associated Security Domain for the Executable Load File;
- At the request of the Security Domain performing the load, request the Security Domain with Receipt Generation privilege to generate a Load Receipt.

At the request of OPEN, the Security Domain with Receipt Generation privilege shall:

- Apply the issuer's policy to generate or not a Load Receipt.

If, at any stage, the OPEN determines that card resources are insufficient for the loading process or that any verification step has failed, the OPEN shall terminate the loading process, shall return the appropriate error and shall reclaim any memory allocated to the load process.

### 9.3.6 Card Content Installation Process

An INSTALL [for install] command is then used to request the installation of an application. The receiving Security Domain processes the INSTALL command before forwarding the install request to the OPEN for processing.

The installation internal processing is beyond the scope of this Specification. However, it is assumed that the installation process includes the creation of instances and allocation of Application data memory.

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0103

Following the installation, the OPEN shall register additional information in the GlobalPlatform Registry regarding the Application Life Cycle State, Security Domain association, and Privileges.

Applications inherit the associated Security Domain of the Executable Load File from which they are installed. They may be extradited to another Security Domain.

The following runtime behavior requirements apply during the content installation process:

**Runtime Behavior (Installation)**

On receipt of the INSTALL [for install] command, the Security Domain performing the installation shall:

- Apply its own secure communication policy;
- Apply its own security policy, e.g. check that its Life Cycle State is PERSONALIZED (only applicable to a Security Domain other than the Issuer Security Domain);
- If the Security Domain performing the installation has the Authorized Management privilege and the off-card entity at the origin of the installation request is not authenticated as its Security Domain Provider (see section 10.4 - *Entity Authentication*), check that an Install Token is present in the INSTALL [for install] command.
- If a Token is present in the INSTALL [for install] command, request the OPEN to obtain verification of the Install Token.
- If the Application Provider identifier is present in the install request, request the OPEN to save this in the GlobalPlatform Registry for the Application.
- Request the OPEN to obtain an Install Receipt.

On receipt of the install request, the OPEN shall:

- Check that the card Life Cycle State is not CARD_LOCKED or TERMINATED;
- Check that OPEN and the requesting on-card entity have no restriction for installation;
- Check that the requesting on-card entity is a Security Domain with Delegated Management or Authorized Management privilege;
- Check that the Executable Module AID is present in the GlobalPlatform Registry;
- Check that the Application AID (for future selection of the Application) is not already present in the GlobalPlatform Registry as an Application or Executable Load File;
- If the Security Domain performing the installation is not the Security Domain associated with the Executable Module from which the Application is being installed, check that the Security Domain associated with the Executable Load File accepts this installation;
- At the request of the Security Domain performing the installation, request the Security Domain with Token Verification privilege to authorize the installation (e.g. to verify the Install Token);
- Verify the resource requirements indicated for the Application (see section 9.7 - *Memory Resource* Management) and that sufficient card resources are available;
- Perform the installation of the Application according to the underlying runtime environment requirements;
- If the Security Domain performing the installation has Delegated Management privilege, ensure that the Security Domain with Token Verification privilege has successfully verified a Token;
- Create an Application from the Executable Module;

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0104

- Ensure that the Application, depending on the underlying runtime environment, has the knowledge of its AID, its Privileges and its Install Parameters;
- Create an entry in the GlobalPlatform Registry for the Application indicating its associated Security Domain, Life Cycle State, Privileges and, when present in the install request, Implicit Selection, Service and Memory Resource Management parameters; and including the Application Provider identifier if supplied by the Security Domain in the installation request;
- At the request of the Security Domain performing the installation, request the Security Domain with Receipt Generation privilege to generate an Install Receipt.

At the request of OPEN, the associated Security Domain shall:

- Apply the Security Domain Provider's policy to accept or reject this installation;
- Apply its own security policy, e.g. check that its Life Cycle State is PERSONALIZED (only applicable to a Security Domain other than the Issuer Security Domain).

At the request of OPEN, the Security Domain with Token Verification privilege shall:

- Verify the Install Token.

At the request of OPEN, the Security Domain with Receipt Generation privilege shall:

- Apply the issuer's policy to generate or not an Install Receipt.

If the OPEN determines that card resources are insufficient for installing the Application or the runtime environment does not currently allow the installation, the OPEN shall terminate the installation process, return the appropriate error and reclaim any memory allocated to the install process.

### 9.3.7 Card Content Make Selectable Process

An INSTALL [for make selectable] command is used to request to make selectable a previously installed application. The receiving Security Domain processes the INSTALL command before forwarding the make selectable request to the OPEN for processing.

The make selectable internal processing is beyond the scope of this Specification.

Following the make selectable, the OPEN shall register additional information in the GlobalPlatform Registry regarding the Application Life Cycle State and Privileges.

The following runtime behavior requirements apply during the content make selectable process:

**Runtime Behavior (Make Selectable)**

On receipt of the INSTALL [for make selectable] command, the Security Domain making the Application selectable shall:

- Apply its own secure communication policy;
- Apply its own security policy, e.g. check that its Life Cycle State is PERSONALIZED (only applicable to a Security Domain other than the Issuer Security Domain);
- If the Security Domain making the Application selectable has the Authorized Management privilege and the off-card entity at the origin of the installation request is not authenticated as its Security Domain Provider (see section 10.4 - *Entity Authentication*), check that a Make Selectable Token is present in the INSTALL [for make selectable] command.
- If a Token is present in the INSTALL [for make selectable] command, request the OPEN to obtain verification of the Make Selectable Token.

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0105

- If the Application Provider identifier is present in the make selectable request, request the OPEN to save this in the GlobalPlatform Registry for the Application.
- Request the OPEN to obtain a Make Selectable Receipt.

On receipt of the make selectable request, the OPEN shall:

- Check that the card Life Cycle State is not CARD_LOCKED or TERMINATED;
- Check that OPEN and the requesting on-card entity have no restriction for make selectable;
- Check that the requesting on-card entity is a Security Domain with Delegated Management or Authorized Management privilege;
- Check that the Application AID is present in the GlobalPlatform Registry;
- If the Security Domain making the Application selectable is not the associated Security Domain of the Application, check that the Security Domain associated with the Application accepts to make it selectable;
- At the request of the Security Domain making the Application selectable, request the Security Domain with Token Verification privilege to authorize the make selectable (e.g. to verify the Make Selectable Token);
- Make the Application selectable according to the underlying runtime environment requirements;
- If the Security Domain making the Application selectable has Delegated Management privilege, ensure that the Security Domain with Token Verification privilege has successfully verified a Token;
- Update accordingly the GlobalPlatform Registry entry for the Application (e.g. Privileges, Implicit Selection parameters);
- At the request of the Security Domain making the Application selectable, request the Security Domain with Receipt Generation privilege to generate a Make Selectable Receipt.

At the request of OPEN, the associated Security Domain shall:

- Apply the Security Domain Provider's policy to accept or reject making this Application selectable;
- Apply its own security policy, e.g. check that its Life Cycle State is PERSONALIZED (only applicable to a Security Domain other than the Issuer Security Domain).

At the request of OPEN, the Security Domain with Token Verification privilege shall:

- Verify the Make Selectable Token.

At the request of OPEN, the Security Domain with Receipt Generation privilege shall:

- Apply the issuer’s policy to generate or not a Make Selectable Receipt.

### 9.3.8 Card Content Combined Loading, Installation and Make Selectable Process

The phases in Figure 9-1 are combined into a single process that uses a combination of multiple occurrences of two different APDU commands (INSTALL and LOAD). The following sequence of APDU commands apply to the loading:

A first INSTALL [for load, install and make selectable] command serves as the combined load and install request for loading and installation. The INSTALL [for load, install and make selectable] command data field details the requirements regarding a Load File.

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0106

Multiple LOAD commands are then used to transport the Load File in blocks according to the size of the file and the communications buffer size of the card.

A last INSTALL [for load, install and make selectable] command serves as the combined load and install commit for loading and installation. The last INSTALL [for load, install and make selectable] command data field details the requirements regarding the Application being installed.

Each INSTALL or LOAD command is processed by the receiving Security Domain before forwarding the load request and Load File Data Block to the OPEN for processing.

The following runtime behavior requirements apply during the content combined loading and installation process.

**Combined Load, Install and Make Selectable Request Runtime Behavior**

On receipt of an INSTALL [for load, install and make selectable] command, the Security Domain performing the combined load and install shall:

- Apply its own secure communication policy;
- Apply its own security policy, e.g. check that its Life Cycle State is PERSONALIZED (only applicable to a Security Domain other than the Issuer Security Domain);
- If a Load File Data Block Hash is present in the INSTALL [for load, install and make selectable] command, request the OPEN to initiate the hash verification of the subsequent Load File Data Block;
- If the Application Provider identifier is present in the load request, request the OPEN to save this in the GlobalPlatform Registry for the Executable Load File.

On receipt of a combined load and installation request (arising from an INSTALL [for load, install and make selectable] command), the OPEN shall:

- Check that the card Life Cycle State is not CARD LOCKED or TERMINATED;
- Check that OPEN and the requesting on-card entity have no restriction for load, installation and make selectable;
- Check that the requesting on-card entity is a Security Domain with Delegated Management or Authorized Management privilege;
- Check that the AID of the Load File is not already present in the GlobalPlatform Registry as an Executable Load File or Application;
- If an associated Security Domain AID is present, and is not the Security Domain performing the combined load, install and make selectable, check that this AID exists within the GlobalPlatform Registry and is registered with the Security Domain privilege. As this equates to the extradition of the Load File, check that the associated Security Domain accepts this extradition and combined load, install and make selectable operation. If no associated Security Domain AID is indicated, the Security Domain performing the load is by default the associated Security Domain.

At the request of OPEN, the associated Security Domain shall:

- Apply the Security Domain Provider's policy to accept or reject this combined load, install and make selectable operation;
- Apply its own security policy, e.g. check that its Life Cycle State is PERSONALIZED (only applicable to a Security Domain other than the Issuer Security Domain).

At the request of OPEN, a Security Domain accepting an implicit extradition shall:

- Apply the Security Domain Provider's policy to accept or reject this implicit extradition;

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0107

- Apply its own security policy, e.g. check that its Life Cycle State is PERSONALIZED (only applicable to a Security Domain other than the Issuer Security Domain).

**Load Phase Runtime Behavior**

On receipt of the LOAD commands, the Security Domain performing the load shall:

- Apply its own secure communication policy;
- Discover whether any Security Domain has the Mandated DAP Verification privilege and if so:
  - Ensure that the required authentication data (DAP Block identifying the above Security Domain) is present in the Load File.
- Check if the associated Security Domain has the DAP Verification privilege and if so:
  - Ensure that the required authentication data (DAP Block identifying the associated Security Domain) is present in the Load File.
- If authentication data (one or more DAP Blocks) is present in the Load File:
  - Ensure that a Load File Data Block Hash was received during the combined load, install and make selectable request process;
  - Extract the authentication data (one or more DAP Blocks) from the Load File;
  - For each DAP Block of the Load File, request the OPEN to obtain verification of the DAP by the Security Domain indicated in the DAP Block.

On receipt of the Load File the OPEN shall:

- Verify the resource requirements of the Load File (see section 9.7- *Memory Resource Management*) and that sufficient card resources are available;
- Check that each DAP verification request from the Security Domain performing the load relates to a Security Domain present in the GlobalPlatform Registry with DAP or Mandated DAP Verification privilege and if so request the Security Domain to verify the DAP;
- Compute the hash of the Load File Data Block when verification of a DAP Block or a combined Load, Install and Make Selectable Token is requested;

At the request of OPEN, the Security Domain(s) verifying the DAP(s) shall:

- Verify that the DAP matches with the Load File Data Block Hash received in the load request.

On completion of the load process the OPEN shall:

- At the request of the Security Domain performing the load, verify the Load File Data Block Hash received in the combined load, install and make selectable request;
- Check in the GlobalPlatform Registry if any Security Domain has the Mandated DAP Verification privilege and if so:
  - Ensure that the above Security Domain has successfully verified a DAP;
- Check in the GlobalPlatform Registry if the associated Security Domain has the DAP Verification privilege and if so:
  - Ensure that the associated Security Domain has successfully verified a DAP;
- If one or more DAP verifications were performed, verify the Load File Data Block Hash received in the load request.

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0108

**Combined Load, Install and Make Selectable Completion Runtime Behavior**

On receipt of the last INSTALL [for load, install and make selectable] command, the Security Domain performing the combined load and install shall:

- Apply its own secure communication policy;
- If the Security Domain performing the installation has the Authorized Management privilege and the off-card entity at the origin of the installation request is not authenticated as its Security Domain Provider (see section 10.4 - *Entity Authentication*), check that a Load, Install and Make Selectable Token is present in the INSTALL [for load, install and make selectable] command;
- If a Token is present in the INSTALL [for load, install and make selectable] command, request the OPEN to obtain verification of the Load, Install and Make Selectable Token;
- If the Application Provider identifier is present in the combined load, install and make selectable request, request the OPEN to save this in the GlobalPlatform Registry for the Executable Load File and the Application;
- Request the OPEN to obtain a combined Load, Install and Make Selectable Receipt.

On completion of the load, install and make selectable process the OPEN shall:

- If the Security Domain performing the combined load, install and make selectable has Delegated Management privilege, ensure that the Security Domain with Token Verification privilege has successfully verified a Token;
- Create an Executable Load File using the Load File Data Block;
- Create an entry in the GlobalPlatform Registry for the Executable Load File indicating its associated Security Domain;
- Create an entry for each Executable Module within the Executable Load File in the GlobalPlatform Registry. This shall include the Application Provider identifier if requested by the Security Domain in the combined load, install and make selectable request. The associated Security Domain for each Executable Module shall be the same as the associated Security Domain for the Executable Load File;
- Check that the Application AID (for future selection of the Application) is not already present in the GlobalPlatform Registry as an Application or Executable Load File;
- Perform the installation of the Application according to the underlying runtime environment requirements;
- Create an Application from the Executable Module;
- Ensure that the Application, depending on the underlying runtime environment, has the knowledge of its AID, its Privileges and its Install Parameters;
- Create an entry in the GlobalPlatform Registry for the Application indicating its associated Security Domain, Life Cycle State, Privileges and, when present in the combined load, install and make selectable request, Implicit Selection, Service and Memory Resource Management parameters; and including the Application Provider identifier if supplied by the Security Domain in the combined load, install and make selectable request;
- At the request of the Security Domain performing the combined load, install and make selectable, request the Security Domain with Token Verification privilege to generate a Load, Install and Make selectable Receipt;
- Verify the resource requirements indicated for the Application (see section 9.7- *Memory Resource Management*) and that sufficient card resources are available.

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0109

At the request of OPEN, the Security Domain with Token Verification privilege shall:

- Verify the combined Load, Install and Make Selectable Token.

At the request of OPEN, the Security Domain with Receipt Generation privilege shall:

- Apply the issuer's policy to generate or not a combined Load, Install and Make Selectable Receipt.

If, at any stage, the OPEN determines that card resources are insufficient for the loading process or that any verification step has failed, the OPEN shall terminate the loading process, shall return the appropriate error and shall reclaim any memory allocated to the load process.

### 9.3.9 Examples of Loading and Installation Flow

The following diagram is an example of the loading and installing of an Application to a GlobalPlatform card. In this example loading and installation are performed by a Security Domain with Authorized Management privilege. The Load File is loaded on the card and stored in memory as an Executable Load File. The installation phase occurs immediately following the loading phase.

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0110

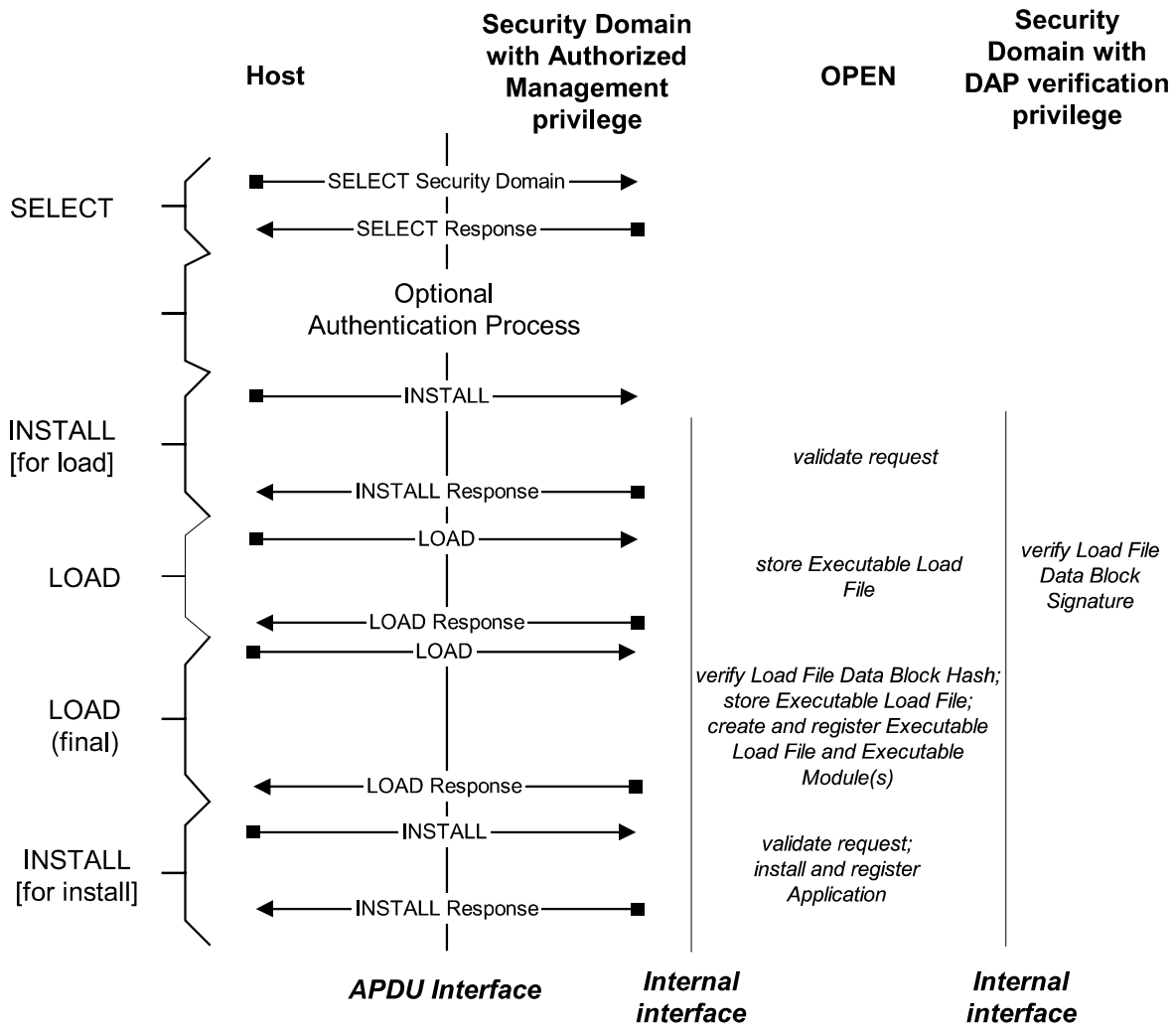



**Figure 9-2: Load and Installation Flow Diagram**

The following diagram is an example of the loading of an Application to a GlobalPlatform card. In this example loading is performed by a Security Domain with Delegated Management privilege.

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0111

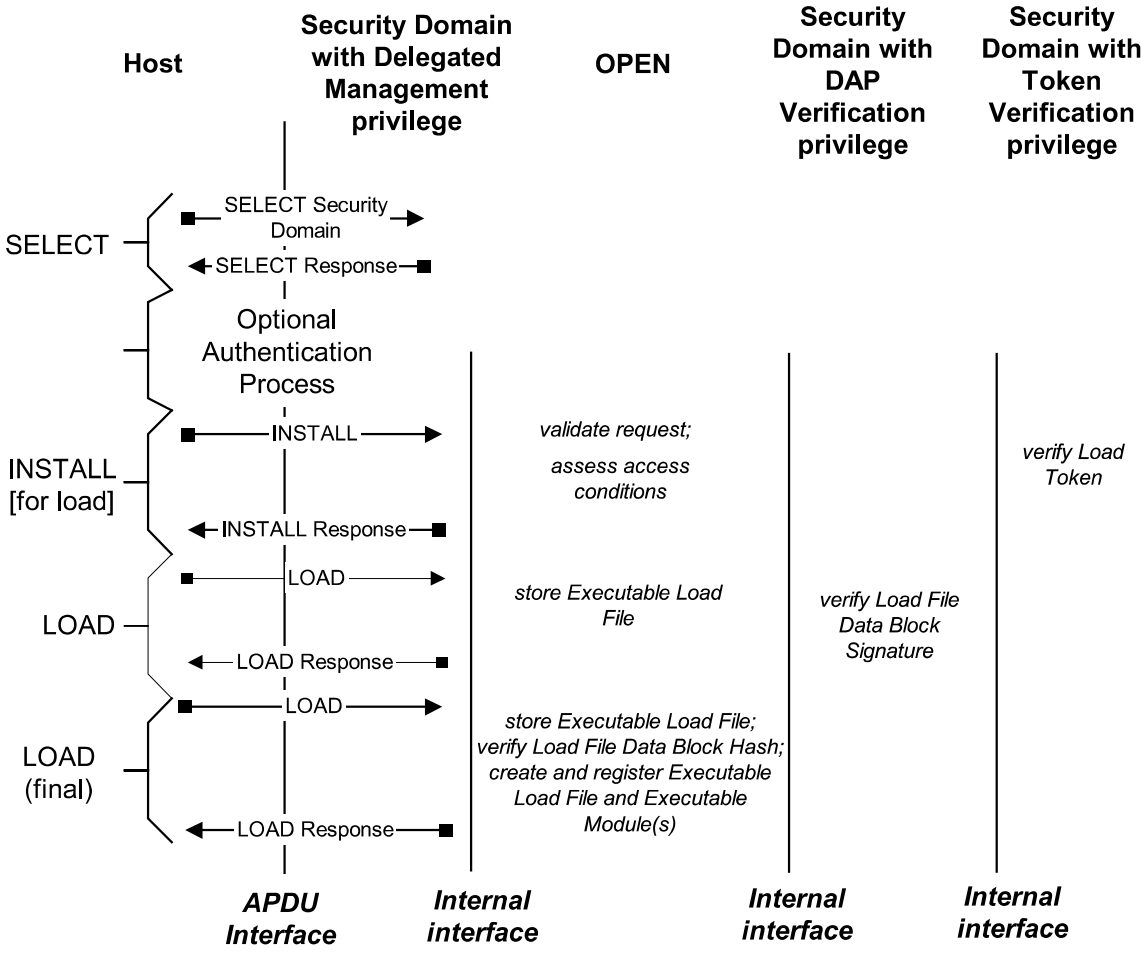



**Figure 9-3: Load Flow Diagram**

The following diagram is an example of installing an Application from an Executable Load File already present on the card. In this example loading and installation are performed by a Security Domain with Delegated Management privilege.

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0112

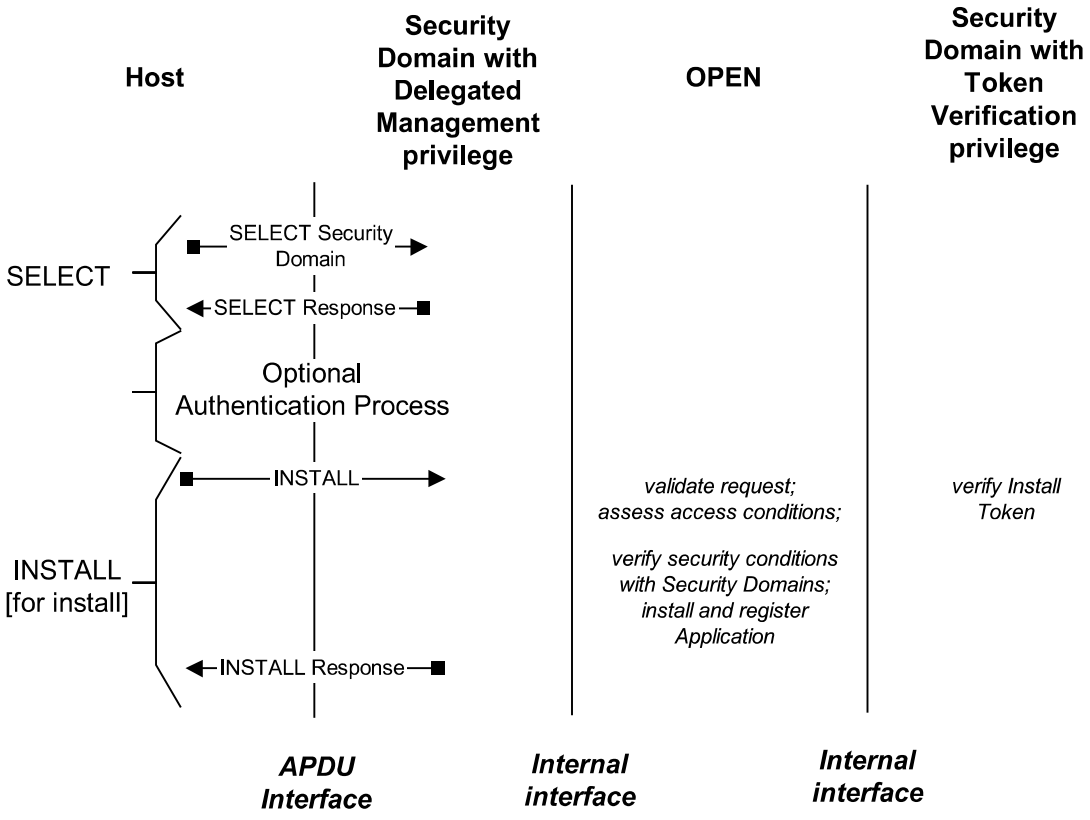



**Figure 9-4: Install Flow Diagram**

## 9.4 Content Extradition and Registry Update

### 9.4.1 Content Extradition

The GlobalPlatform Card Content extradition process is designed to allow a previously installed Application or a previously loaded Executable Load File to be associated with a different Security Domain.

Delegated Extradition allows an Application Provider to extradite one of its Applications to another Security Domain, if the current Security Domain has Delegated Management privilege.

The extradition may apply at any time during the Application Life Cycle. Extradition may apply for any Security Domain (in the PERSONALIZED state) or the Issuer Security Domain (in any card Life Cycle State other than CARD_LOCKED and TERMINATED), that accepts the extradited Application.

The extradition process comprises an INSTALL [for extradition] command processed by the receiving Security Domain. The Security Domain then passes the extradition request to the OPEN for additional verification and processing.

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0113

The Extradition Token allows the OPEN, via the Security Domain with Token Verification privilege within the same sub-hierarchy as the Security Domain performing the extradition, to ensure that the token authorized the extradition process.

The response to the INSTALL [for extradition] command identifies the end of the extradition process. Following the completion of the extradition process, an optional Extradition Receipt is returned to the Security Domain performing the Delegated Management operation and shall be transmitted by the Security Domain to the off-card entity.

The Application Provider may then forward the Extradition Receipt to the corresponding off-card entity as a proof that the extradition process was successfully performed. The purpose of the optional Extradition Receipt is to assist the Application Provider in keeping its Card Management System synchronized with its on-card application base.

The following runtime behavior requirements apply during the Card Content extradition process.

**Runtime Behavior**

On receipt of the INSTALL [for extradition] command, the Security Domain performing the extradition shall:

- Apply its own secure communication policy;
- Apply its own security policy, e.g. check that its Life Cycle State is PERSONALIZED (only applicable to a Security Domain other than the Issuer Security Domain);
- If the Security Domain performing the extradition has the Authorized Management privilege and the off-card entity at the origin of the extradition request is not authenticated as its Security Domain Provider (see section 10.4 - *Entity Authentication*), check that an Extradition Token is present in the INSTALL [for extradition] command;
- If a Token is present in the INSTALL [for extradition] command, request the OPEN to obtain verification of the Extradition Token;
- Request the OPEN to obtain an Extradition Receipt.

On receipt of an extradition request, the OPEN shall:

- Check that the card Life Cycle State is not CARD_LOCKED or TERMINATED;
- Check that OPEN and the requesting on-card entity have no restriction for extradition;
- Determine if the Application or Executable Load File being extradited exists within the GlobalPlatform Registry;
- Check that the requesting on-card entity is a Security Domain with Delegated Management or Authorized Management privilege;
- Check that an on-card entity with the same AID as the Security Domain to which the Application or Executable Load File is being extradited exists within the GlobalPlatform Registry, and that this on-card entity has the Security Domain privilege;
- If the Security Domain performing the extradition has the Delegated Management privilege, ensure that the Security Domain with Token Verification privilege has successfully verified a Token;
- Update accordingly the GlobalPlatform Registry entry for the Application or Executable Load File;
- At the request of the Security Domain performing the extradition, request the Security Domain with Receipt Generation privilege to generate an Extradition Receipt.

At the request of OPEN, the currently associated Security Domain shall:

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0114

- Apply the Security Domain Provider's policy to accept or reject this extradition request;
- Apply its own security policy, e.g. check that its Life Cycle State is PERSONALIZED (only applicable to a Security Domain other than the Issuer Security Domain).

At the request of OPEN, the Security Domain with Token Verification privilege shall:

- Verify the Extradition Token.

At the request of OPEN, the Security Domain with Receipt Generation privilege shall:

- Apply the issuer's policy to generate or not an Extradition Receipt.

At the request of OPEN, the Security Domain accepting the explicit extradition shall:

- Apply the Security Domain Provider's policy to accept or reject this Card Content extradition;
- Apply its own security policy, e.g. check that its Life Cycle State is PERSONALIZED (only applicable to a Security Domain other than the Issuer Security Domain).

The Security Domain requesting the extradition does not need to be associated with the Application or Load File being extradited. The Security Domain initially associated with the Application may accept or reject the extradition as detailed in a configuration.

### Extradition Flow

The following figure is an example of extradition, and shows delegated extradition:

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0115

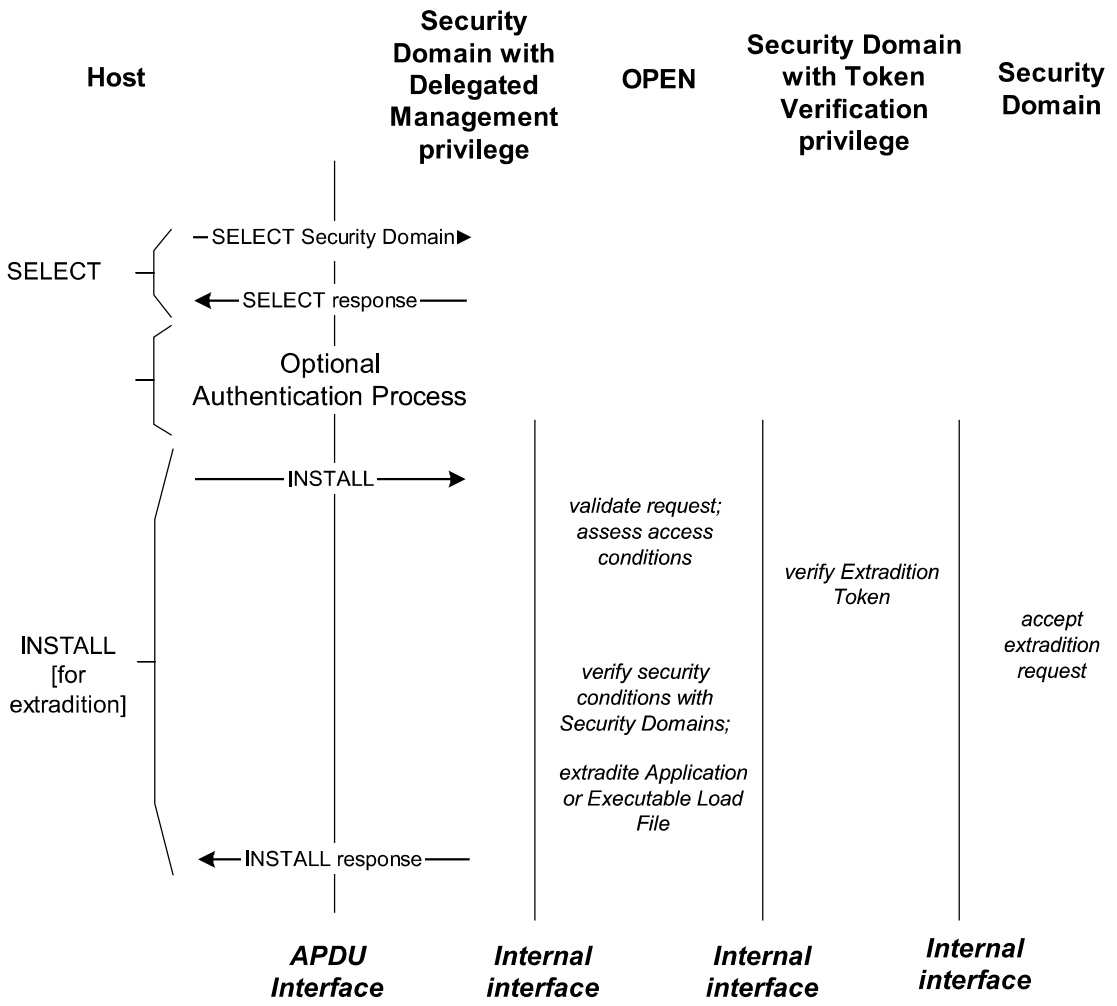



**Figure 9-5: Delegated Extradition Flow**

## 9.4.2 Registry Update

### 9.4.2.1 Generic Registry Update

The registry update process allows GlobalPlatform Registry data associated with an Application, such as Privileges and Implicit Selection parameters, to be modified. This process also allows the restricting of Card Content Management functionality of a specific Security Domain or OPEN itself (i.e. of all existing Security Domains present on the card and any eventual Security Domain installed afterwards).

The registry update may apply at any time during the Application Life Cycle or card Life Cycle (other than CARD_LOCKED or TERMINATED).

The registry update process comprises one or more INSTALL [for registry update] commands processed by the receiving Security Domain. To restrict Card Content Management functionality of OPEN, no Application AID is provided in the INSTALL [for registry update] command. The Security Domain then passes the registry update request to the OPEN for additional verification and processing.

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0116

The Registry Update Token allows the OPEN, via the Security Domain with Token Verification privilege within the same sub-hierarchy as the Security Domain performing the Registry Update, to ensure that the token authorizes the update of the GlobalPlatform Registry.

The response to the INSTALL [for registry update] command identifies the end of the registry update process. Following the completion of the registry update process, an optional Registry Update Receipt is returned to the Security Domain performing the Delegated Management operation and shall be transmitted by the Security Domain to the off-card entity.

The Application Provider may then forward the Registry Update Receipt to the corresponding off-card entity as a proof that the registry update process was successfully performed. The purpose of the optional Registry Update Receipt is to assist the Application Provider in keeping its Card Management System synchronized with its on-card application base.

The following runtime behavior requirements apply during the registry update process.

**Runtime Behavior**

On receipt of the INSTALL [for registry update] command, the Security Domain performing the registry update shall:

- Apply its own secure communication policy;
- Apply its own security policy, e.g. check that its Life Cycle State is PERSONALIZED (only applicable to a Security Domain other than the Issuer Security Domain);
- If the Security Domain performing the registry update has the Authorized Management privilege and the off-card entity at the origin of the registry update request is not authenticated as its Security Domain Provider (see section 10.4 - *Entity Authentication*), check that a Registry Update Token is present in the INSTALL [for registry update] command;
- If a Token is present in the INSTALL [for registry update] command, request the OPEN to obtain verification of the Registry Update Token;
- Request the OPEN to obtain a Registry Update Receipt.

On receipt of a registry update request, the OPEN shall:

- Check that the card Life Cycle State is not CARD_LOCKED or TERMINATED;
- Check that OPEN and the requesting on-card entity have no restriction for registry update;
- When updating an Application, determine if the Application being updated exists within the GlobalPlatform Registry;
- Check that the requesting on-card entity is a Security Domain with Delegated Management or Authorized Management privilege;
- When restricting functionality of OPEN, check that the requesting on-card entity is a Security Domain with Global Lock privilege;
- If the Security Domain requesting the registry update is not the associated Security Domain of the Application, check that the Security Domain associated with the Application accepts this registry update;
- If the Security Domain performing the registry update has the Delegated Management privilege, ensure that the Security Domain with Token Verification privilege has successfully verified a Token;
- Update accordingly the GlobalPlatform Registry entry for the Application being updated;

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0117

- At the request of the Security Domain performing the registry update, request the Security Domain with Receipt Generation privilege to generate a Registry Update Receipt.

At the request of OPEN, the associated Security Domain shall:

- Apply the Security Domain Provider's policy to accept or reject this registry update;
- Apply its own security policy, e.g. check that its Life Cycle State is PERSONALIZED (only applicable to a Security Domain other than the Issuer Security Domain).

At the request of OPEN, the Security Domain with Token Verification privilege shall:

- Verify the Registry Update Token.

At the request of OPEN, the Security Domain with Receipt Generation privilege shall:

- Apply the issuer's policy to generate or not a Registry Update Receipt.

#### 9.4.2.2 Extradition using Registry Update

An extradition may be performed using the registry update process. The simultaneous extradition and registry update process is achieved by an appropriately formed INSTALL [for registry update] command.

The runtime behavior requirements for an extradition using registry update are the sum of the runtime behavior requirements for general registry update as well as the additional runtime behavior requirements specified below.

If a Token is required the Registry Update Token is used, and if a Receipt is to be returned the Registry Update Receipt is used; both of which allow for extradition as well as for registry update.

**Additional Runtime Behavior**

At the request of the OPEN, the Security Domain accepting the explicit extradition shall:

- Apply the Security Domain Provider's policy to accept or reject this Card Content extradition;
- Apply its own security policy, e.g. check that its Lifecycle State is PERSONALIZED (only applicable to a Security Domain other than the Issuer Security Domain).

## 9.5 Content Removal

This section defines the content removal process that enables a flexible management of the Mutable Persistent Memory space of the cards through the removal of Applications and/or Executable Load Files. Only code and data not referenced by another entity on the card may be deleted. Code and data that is currently being accessed by the runtime environment is deemed to be referenced by another entity. If the Application is selected on another logical channel this Application cannot be deleted.

The DELETE command (see section 11.2 - *DELETE Command*) allows for the actual removal of content from Mutable Persistent Memory and the logical removal of content from Immutable Persistent Memory. The DELETE command is processed by the receiving Security Domain before forwarding the removal request to the OPEN for processing.

Depending on the memory location of the removed Applications and/or Executable Load File, the OPEN shall perform the different actions detailed in the following sections. When the Application or Executable Load File has been successfully removed, its contents in the memory shall no longer be accessible.

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0118

A Security Domain with Global Delete privilege has the privilege to delete any Application or Executable Load File from the card regardless of which Security Domain the Application or Executable Load File is associated with.

The Delete Token allows the OPEN, via the Security Domain with the Token Verification privilege within the same sub-hierarchy as the Security Domain performing the Delete, to ensure that the token authorizes the deletion of the associated GlobalPlatform Registry entries.

The response to the DELETE command identifies the end of the deletion process. Following the completion of the deletion process, an optional Delete Receipt is returned to the Security Domain performing the Delegated Management operation and shall be transmitted by the Security Domain to the off-card entity.

The Application Provider may then forward the Delete Receipt to the corresponding off-card entity as a proof that the deletion process was successfully performed. The purpose of the optional Delete Receipt is to assist the Application Provider in keeping its Card Management System synchronized with its on-card application base.

**Deletion Flow**

The following figure is an example of deleting an Application, an Executable Load File, or both:

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0119

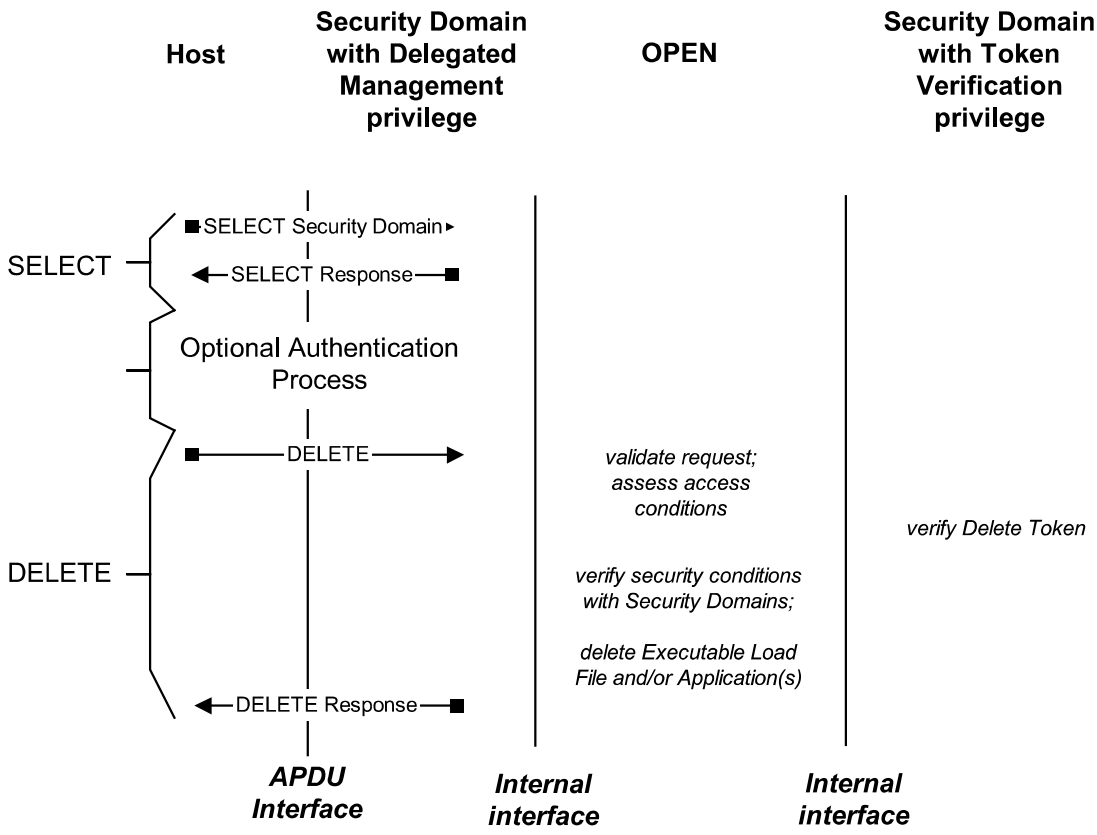



**Figure 9-6: Content Deletion Flow**

### 9.5.1 Application Removal

Application removal may involve the removal of Application instances as well as any Application data associated with the Application.

The following runtime behavior requirements apply during the Application removal process.

#### Runtime Behavior

On receipt of an Application deletion request (DELETE command), the Security Domain performing the deletion shall:

- Apply its own secure communication policy;
- Apply its own security policy, e.g. check that its Life Cycle State is PERSONALIZED (applicable to a Security Domain other than the Issuer Security Domain);
- If the Security Domain performing the deletion has the Authorized Management privilege and the off-card entity at the origin of the delete request is not authenticated as its Security Domain Provider (see section 10.4 - *Entity Authentication*), check that a Delete Token is present in the DELETE command;

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0120

- If a Token is present in the DELETE command, request the OPEN to obtain verification of the Delete Token;
- Request the OPEN to obtain a Delete Receipt.

On receipt of an Application deletion request, the OPEN shall:

- Check that the card Life Cycle State is not CARD_LOCKED or TERMINATED;
- Check that OPEN and the requesting on-card entity have no restriction for deletion;
- Determine that the Application being deleted has an entry within the GlobalPlatform Registry;
- Check that the requesting on-card entity is a Security Domain with Delegated Management or Authorized Management privilege;
- Check that the Security Domain performing the deletion is the associated Security Domain of the Application being deleted, or that it has Global Delete privilege. Otherwise (i.e. if the Security Domain performing the deletion is not associated with the Application being deleted and does not have the Global Delete privilege), check that the Security Domain associated with the Application accepts this deletion;
- At the request of the Security Domain performing the deletion, request the Security Domain with Token Verification privilege to verify the Delete Token;
- Determine that the Application is not currently selected on another logical channel;
- Determine that no other Applications present in the card make references to this Application;
- Determine that no other Applications present in the card make references to any data within this Application;
- If a Security Domain is being deleted, determine that none of the Applications or Executable Load Files present in the card are associated with this Security Domain;
- If the Security Domain performing the deletion has the Delegated Management privilege, ensure that the Security Domain with Token Verification privilege has successfully verified a token;
- Remove the entry for the Application from within the GlobalPlatform Registry;
- Re-assign the Application's privileges (if any) to the Issuer Security Domain as defined in section 6.6.2 - *Privilege Assignment*;
- If the Application is implicitly selectable, re-assign implicit selection to the Issuer Security Domain as defined in section 6.4.1 - *Implicit Selection Assignment*;
- Release and mark as available any Mutable Persistent Memory and when supported, apply the memory resource management rules described in section 9.7 - *Memory Resource Management*;
- At the request of the Security Domain performing the deletion, request the Security Domain with Receipt Generation privilege to generate a Delete Receipt.

If the OPEN determines that any of the above verification steps have failed, the OPEN shall not initiate the delete process and shall inform the Security Domain to return the appropriate response. Once this delete process begins it shall complete in the current Card Session or, in the event of an interruption, at least the updates to the GlobalPlatform Registry shall complete in a subsequent Card Session.

At the request of OPEN, the associated Security Domain shall:

- Apply the Security Domain Provider's security policy to accept or reject this Application removal;
- Apply its own security policy e.g. check that its Life Cycle State is PERSONALIZED (only applicable to a Security Domain other than the Issuer Security Domain).

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0121

At the request of OPEN, the Security Domain with Token Verification privilege shall:

- Apply the issuer's policy to accept or reject a deletion authorization request without the presence of a Delete Token;
- Verify the Delete Token.

At the request of OPEN, the Security Domain with Receipt Generation privilege shall:

- Apply the issuer's policy to generate or not a Delete Receipt.

### 9.5.2 Executable Load File Removal

An Executable Load File contains Executable Modules. The removal applies to the entire Executable Load File. Physical removal may occur in Mutable Persistent Memory while only logical removal is possible in Immutable Persistent Memory.

This version of the Specification does not cover the removal of a specific Executable Module within an Executable Load File.

The following runtime behavior requirements apply during the Executable Load File removal process.

#### Runtime Behavior

On receipt of an Executable Load File deletion request (DELETE command), the Security Domain performing the deletion shall:

- Apply its own secure communication policy;
- Apply its own security policy, e.g. check that its Life Cycle State is PERSONALIZED (only applicable to a Security Domain other than the Issuer Security Domain);
- If the Security Domain performing the deletion has the Authorized Management privilege and the off-card entity at the origin of the delete request is not authenticated as its Security Domain Provider (see section 10.4 - *Entity Authentication*), check that a Delete Token is present in the DELETE command;
- If a Token is present in the DELETE command, request the OPEN to obtain verification of the Delete Token;
- Request the OPEN to obtain a Delete Receipt.

On receipt of an Executable Load File removal process deletion request, the OPEN shall:

- Check that the card Life Cycle State is not CARD_LOCKED or TERMINATED;
- Check that OPEN and the requesting on-card entity have no restriction for deletion;
- Check that the requesting on-card entity is a Security Domain with Delegated Management or Authorized Management privilege;
- Check that the Security Domain performing the deletion is the associated Security Domain of the Executable Load File being deleted, or that it has Global Delete privilege. Otherwise (i.e. if the Security Domain performing the deletion is not associated with the Executable Load File being deleted and does not have the Global Delete privilege) check that the Security Domain associated with the Executable Load File accepts this deletion;
- At the request of the Security Domain performing the deletion, request the Security Domain with Token Verification privilege to verify the Delete Token;

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0122

- Determine that the Executable Load File being deleted has an entry within the GlobalPlatform Registry;
- Determine that no other Applications and no other Executable Load Files present in the card maintain references to this Executable Load File;
- If the Security Domain performing the deletion has the Delegated Management privilege, ensure that the Security Domain with Token Verification privilege has successfully verified a Token;
- Remove the entry for the Executable Load File and the entries for any Executable Modules present in the Executable Load File from within the GlobalPlatform Registry;
- Release and mark as available any Mutable Persistent Memory and when supported, apply the memory resource management rules described in section 9.7 - *Memory Resource Management*;
- At the request of the Security Domain performing the deletion, request the Security Domain with Receipt Generation privilege to generate a Delete Receipt.

If the OPEN determines that any of the above verification steps have failed, the OPEN shall not initiate the delete process and shall inform the Security Domain to return the appropriate response. Once this delete process begins it shall all complete in the current Card Session or, in the event of an interruption, at least the updates to the GlobalPlatform Registry shall complete in a subsequent Card Session.

Only Mutable Persistent Memory is released and marked as available. Executable Load Files contained in Immutable Persistent Memory cannot be deleted but the entry for the Executable Load File and the entries for the Executable Modules present in the Executable Load File shall be deleted from the GlobalPlatform Registry.

At the request of OPEN, the associated Security Domain shall:

- Apply the Security Domain Provider's policy to accept or reject this Executable Load File removal;
- Apply its own security policy, e.g. check that its Life Cycle State is PERSONALIZED (only applicable to a Security Domain other than the Issuer Security Domain).

At the request of OPEN, the Security Domain with Token Verification privilege shall:

- Apply the issuer’s policy to accept or reject a deletion authorization request without the presence of a Delete Token;
- Verify the Delete Token.

At the request of OPEN, the Security Domain with Receipt Generation privilege shall:

- Apply the issuer’s policy to generate or not a Delete Receipt.

### 9.5.3 Executable Load File and related Application Removal

An Executable Load File contains Executable Modules from which Applications have been installed. This optional feature removes the Executable Load File as well as all these related Applications. Physical removal may occur in Mutable Persistent Memory while only logical removal is possible in Immutable Persistent Memory.

When supported by the card, the following runtime behavior requirements apply during the Executable Load File and related Application removal process.

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0123

**Runtime Behavior**

On receipt of an Executable Load File deletion request (DELETE command), the Security Domain performing the deletion shall:

- Apply its own secure communication policy;
- Apply its own security policy, e.g. check that its Life Cycle State is PERSONALIZED (only applicable to a Security Domain other than the Issuer Security Domain);
- If the Security Domain performing the deletion has the Authorized Management privilege and the off-card entity at the origin of the delete request is not authenticated as its Security Domain Provider (see section 10.4 - *Entity Authentication*), check that a Delete Token is present in the DELETE command;
- If a Token is present in the DELETE command, request the OPEN to obtain verification of the Delete Token;
- Request the OPEN to obtain a Delete Receipt.

On receipt of a request to remove an Executable Load File and its related Applications, the OPEN shall:

- Check that the card Life Cycle State is not CARD_LOCKED or TERMINATED;
- Check that OPEN and the requesting on-card entity have no restriction for deletion;
- Check that the requesting on-card entity is a Security Domain with Delegated Management or Authorized Management privilege;
- Check that the Security Domain performing the deletion is the associated Security Domain of each of the related Applications being deleted, or that it has the Global Delete privilege. Otherwise (i.e. if the Security Domain performing the deletion is not associated with one or more of the Applications being deleted and does not have the Global Delete privilege) check in each case that the Security Domain associated with the related Application accepts this deletion;
- Check that the Security Domain performing the deletion is the associated Security Domain of the Executable Load File being deleted, or that it has the Global Delete privilege. Otherwise (i.e. if the Security Domain performing the deletion is not associated with the Executable Load File being deleted and does not have the Global Delete privilege) check that the Security Domain associated with the Executable Load File accepts this deletion;
- At the request of the Security Domain performing the deletion, request the Security Domain with Token Verification privilege to verify the Delete Token;
- If the Security Domain performing the deletion has the Delegated Management privilege, ensure that the Security Domain with Token Verification privilege has successfully verified a Token;
- Determine that the Executable Load File and Applications being deleted have entries within the GlobalPlatform Registry;
- Locate each Application installed from an Executable Module within this Executable Load File and for each Application:
  - Determine that the Application is not currently selected on another logical channel;
  - Determine that no other non-related Applications present in the card make reference to this Application;
  - Determine that no other non-related Applications present in the card maintain references to any data within this Application;

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0124

  - If a Security Domain is being deleted, determine that none of the non-related Applications present in the card are associated with this Security Domain;

- Determine that no other Applications and no other Executable Load Files present in the card maintain references to this Executable Load File;
- Remove the entry for the Executable Load File and the entries for any Executable Modules present in the Executable Load File from within the GlobalPlatform Registry;
- Remove the entry for each related Application within the GlobalPlatform Registry;
- Re-assign the privileges of all related Applications (if any) to the Issuer Security Domain as defined in section 6.6.2 - *Privilege Assignment*;
- If any related Application is implicitly selectable, re-assign implicit selection to the Issuer Security Domain as defined in section 6.4.1 - *Implicit Selection Assignment*;
- Release and mark as available any Mutable Persistent Memory and when supported, apply the memory resource management rules described in section 9.7 - *Memory Resource Management*;
- At the request of the Security Domain performing the deletion, request the Security Domain with Receipt Generation privilege to generate a Delete Receipt.

If the OPEN determines that any of the above verification steps have failed, the OPEN shall not initiate the delete process and shall inform the Security Domain to return the appropriate response. Once the delete processes begin they shall all complete in the current Card Session or, in the event of an interruption, at least the updates to the GlobalPlatform Registry shall complete in a subsequent Card Session.

Only Mutable Persistent Memory is released and marked as available. Executable Load Files contained in Immutable Persistent Memory cannot be deleted but the entry for the Executable Load File and the entries for the Executable Modules present in the Executable Load File shall be deleted from the GlobalPlatform Registry.

At the request of OPEN, the associated Security Domain shall:

- Apply the Security Domain Provider's policy to accept or reject this Executable Load File and related Application removal;
- Apply its own security policy, e.g. check that its Life Cycle State is PERSONALIZED (only applicable to a Security Domain other than the Issuer Security Domain).

At the request of OPEN, the Security Domain with Token Verification privilege shall:

- Apply the issuer’s policy to accept or reject a deletion authorization request without the presence of a Delete Token;
- Verify the Delete Token.

At the request of OPEN, the Security Domain with Receipt Generation privilege shall:

- Apply the issuer’s policy to generate or not a Delete Receipt.

## 9.6 Security Management

### 9.6.1 Life Cycle Management

The following set of services is provided to manage the Life Cycles of on-card entities:

- Application locking and unlocking;

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0125

- Card locking and unlocking;
- Card termination;
- Application Life Cycle interrogation;
- Card Life Cycle interrogation.

**Life Cycle Management Flow**

Figure 9-7 shows the flow that is common to all the Life Cycle management services:

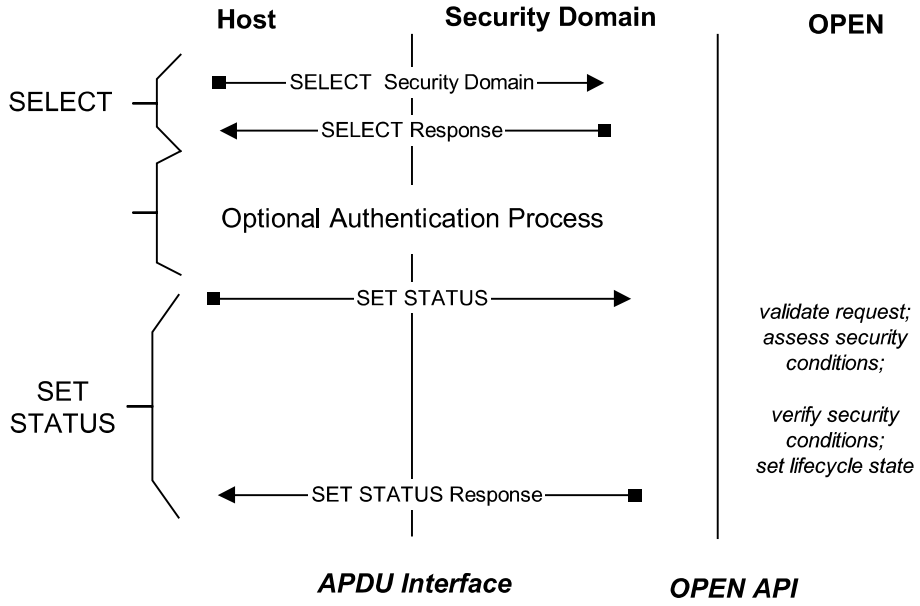



**Figure 9-7: Life Cycle Management Flow**

## 9.6.2 Application Locking and Unlocking

The card has a mechanism to disable and subsequently re-enable the continued execution status of an on-card Application. This mechanism may be invoked from within the OPEN based on exceptions handled by the OPEN or from the use of externally invoked commands. An Application with Global Lock privilege, the Application itself or a directly or indirectly associated Security Domain are the only entities that may initiate the locking of an Application. Only an Application with Global Lock privilege or a directly or indirectly associated Security Domain may initiate the unlocking of an Application.

**Runtime Behavior**

On receipt of a SET STATUS command, the Security Domain performing the lifecycle management shall:

- Apply its own secure communication policy;
- Check that the off-card entity at the origin of the lock/unlock request is authenticated as the Application Provider of the target Application or as the Security Domain Provider (see section 10.4 - *Entity Authentication*).

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0126

On receipt of a request to lock or unlock an Application, the OPEN shall:

- Check that the requesting on-card entity is the Application itself, or the Security Domain directly or indirectly associated with the Application being locked or unlocked, or that the requesting entity has the Global Lock privilege;
- Check that the Application is not requesting to unlock itself;
- Check that an entry for the Application being locked or unlocked is present in the GlobalPlatform Registry and does not have the Final Application privilege;
- For locking, set the Application Life Cycle State to LOCKED;
- For unlocking, reverse the Application Life Cycle State to its previous state;
- For locking, keep a record of the previous Application Life Cycle State to ensure that the Application Life Cycle State can be transitioned back to and only to this previous state.

An Application being locked that is currently selected on a logical channel shall remain the currently selected Application on that logical channel until the end of the Application Session though its Application Life Cycle State is set to LOCKED.

Once the Application Life Cycle State is set to LOCKED, the Application shall not be selectable implicitly or explicitly on any logical channel.

If the locked Application is implicitly selectable on any card interface(s) and logical channel(s), the application with Final Application privilege will be implicitly selected for those card interface(s) and logical channel(s).

### 9.6.3 Card Locking and Unlocking

Once the card Life Cycle State is CARD_LOCKED, all Applications except the Application with the Final Application privilege shall be disabled. Due to the severity of this action, the card locking shall only be allowed under the most stringent conditions and shall only be performed with the proper security mechanisms and authorizations.

Card locking requests may originate from two sources:

**Internal source—** either the OPEN, the Issuer Security Domain, or a privileged Application may initiate card locking requests from within the card. Internal requests are likely to occur in response to certain card runtime situations. For example, the OPEN or an Application with the necessary privilege may initiate the card locking process as a response to a perceived security threat based on data collected from velocity checking data.

**Off-card source—** explicit card locking requests may be initiated by APDU commands sent by the Card Issuer to the Issuer Security Domain or by an authorized representative to an Application with the Card Lock Privilege.

#### Runtime Behavior

On receipt of a SET STATUS command, the Security Domain performing the lifecycle management shall:

- Apply its own secure communication policy;
- Check that the off-card entity at the origin of the lock/unlock request is authenticated as the Security Domain Provider (see section 10.4 - *Entity Authentication*).

On receipt of a request to lock the card, the OPEN shall:

- Check that the requesting on-card entity has the required Card Lock privilege;

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0127

- Check that the current card Life Cycle State is SECURED;
- Set the card Life Cycle State to CARD_LOCKED.

On receipt of a request to unlock the card, the OPEN shall:

- Check that the requesting on-card entity has the required Card Lock privilege;
- Reverse the card Life Cycle State to SECURED.

Applications that are currently selected on any logical channel shall remain the currently selected Applications on their respective logical channels until the end of their respective Application Sessions. As soon as the current Application Session on a Supplementary Logical Channel ends, the logical channel on which the Application was selected is closed. Once all the Supplementary Logical Channels are closed the Basic Logical Channel becomes the only available interface. As soon as the current Application Session on the Basic Logical Channel ends, the Application with the Final Application privilege is the only selectable Application.

Attempts to modify Card Content are denied from the instant the card transitions to the CARD_LOCKED Life Cycle State.

### 9.6.4 Card Termination

In the card Life Cycle State TERMINATED, all communication to the card are directed to the application with the Final Application privilege. If the Issuer Security Domain is the application with this privilege all commands except the GET DATA command processed by the Issuer Security Domain shall be disabled. Due to the severity of this action, the card termination shall only be allowed under the most stringent conditions and shall only be performed with the proper security mechanisms and authorizations.

The decision to terminate a card may either be triggered by an internal card event that violates a policy of the Card Issuer or may be invoked externally:

**Internal source—** either the OPEN, the Issuer Security Domain, or a privileged Application may initiate a card termination request from within the card. An internal card termination request is likely to occur in response to certain card runtime situations.

**Off-card source—** explicit card termination requests can be initiated by APDU commands sent by the Card Issuer to the Issuer Security Domain or by an authorized representative to an Application with the Card Terminate privilege.

#### Runtime Behavior

On receipt of a SET STATUS command, the Security Domain performing the lifecycle management shall:

- Apply its own secure communication policy;
- Check that the off-card entity at the origin of the termination request is authenticated as the Security Domain Provider (see section 10.4 - *Entity Authentication*).

On receipt of a request to terminate the card, the OPEN shall:

- Check that the requesting on-card entity has the Card Terminate privilege;
- Set the card Life Cycle State to TERMINATED from its current state.

Applications that are currently selected on any logical channel shall remain the currently selected Applications on their respective logical channels until the end of their respective Application Sessions. As soon as the current Application Session on a Supplementary Logical Channel ends, the logical channel on which the Application was selected is closed. Once all the Supplementary Logical Channels are closed the Basic Logical Channel becomes the only available interface. As soon as the current Application

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0128

Session on the Basic Logical Channel ends, no Applications are selectable, the Application with Final Application privilege is always implicitly selected on the Basic Logical Channel.

As the transition to the TERMINATED Life Cycle State can be due to the detection of a severe security threat, the security policy of the Issuer may require additional behavior such as closing the current Card Session by performing an internal card reset.

Card Content management requests are denied from the instant the card transitions to the TERMINATED Life Cycle State. Depending on the security policy of the Issuer, other operations may be allowed to continue during the remaining current Application Sessions.

### 9.6.5 Application Status Interrogation

The status of an Application (or a Security Domain): its Life Cycle State, Privileges and other parameters registered in the GlobalPlatform Registry, may be accessed by suitably authorized entities.

#### Runtime Behavior

On receipt of a GET STATUS command, the Security Domain performing the lifecycle interrogation shall:

- Apply its own secure communication policy;
- Check that the off-card entity at the origin of the request is authenticated as the Application Provider of the interrogated Application or as the Security Domain Provider (see section 10.4 - *Entity Authentication*).

On receipt of a request to interrogate the status of an Application, the OPEN shall:

- Check that the requesting on-card entity is the entity itself being interrogated, a Security Domain directly or indirectly associated with the Application being interrogated, or that the requesting entity has the Global Registry privilege

### 9.6.6 Card Status Interrogation

The status of the card and the Issuer Security Domain: its AID, Privileges and other parameters registered in the GlobalPlatform Registry, may be accessed by suitably authorized entities.

#### Runtime Behavior

On receipt of a GET STATUS command, the Security Domain performing the lifecycle interrogation shall:

- Apply its own secure communication policy;
- Check that the off-card entity at the origin of the request is authenticated as the Security Domain Provider (see section 10.4 - *Entity Authentication*).

On receipt of a request to interrogate the card Life Cycle State, the OPEN shall respond.

### 9.6.7 Operational Velocity Checking

The OPEN shall be implemented with a velocity checking security mechanism. For the purpose of this document, “velocity checking” is defined as the active monitoring, handling and management of security sensitive activities on the card.

These activities may include, but are not limited to the following:

- Content installation;
- Card exceptions;

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0129

- Application exceptions.

Typically, velocity checking is used to counter security attacks that use repeated attempts in their schemes. These attempts can be from internal (on-card) or external (off-card) entities. Velocity checking is implemented to track the number of consecutive failures in each of the related management and security events.

#### 9.6.7.1 Content Loading and Installation

The OPEN may keep track of the number of unsuccessful consecutive attempts of the Card Content load and installation process by a particular Application and the total number of such attempts by all Applications. Actions may include such defensive measures as the locking or termination of the card.

#### 9.6.7.2 Exceptions

Velocity checking may be implemented in cases in which the OPEN generates exceptions. However, it does not have to be implemented such that each individual exception is handled separately. A trace buffer and event log may be used to complement velocity checking.

For example, an implementation of a Security Domain may enable velocity checking to enforce strict APDU command sequencing for card and application management operations (e.g., Card Content loading and installation). The OPEN may also enable velocity checking against repeated failed attempts by an Application to allocate additional memory beyond its allowed limit that is stored in the GlobalPlatform Registry. The OPEN may choose to lock an Application that is exhibiting such behavior.

### 9.6.8 Tracing and Event Logging

Tracing and event logging functions may be enabled. These functions shall be implemented according to a Card Issuer's policy requirements.

## 9.7 Memory Resource Management

Memory resource management is an optional feature of a GlobalPlatform card. It consists of the management by OPEN of counters associated with Executable Load Files or Applications regarding their individual allocation of memory resources, as defined in this specification. It applies to both persistent and volatile memory. Memory resource management data elements describe memory usage requirements applicable to each type of memory: volatile or persistent; and for each type of storage: code or data. Memory requirements may be defined for each Executable Load File and Application at the time of their load and installation. The OPEN, in conjunction with the Runtime Environment, is responsible for managing the memory resources of the card; including the security requirements defined in section 4.2.4.1 - *Runtime Environment Security Requirements*.

A memory resource management data element indicates an amount of memory resources in bytes. In the INSTALL [for load] command, the System Parameters may include memory requirements specifying for each type of memory a Minimum Memory, or Reserved Memory, or both data elements. In the INSTALL [for install] command, the System Parameters may include memory requirements specifying for each type of memory a Memory Quota, or Reserved Memory, or both.

When memory resource management is supported, the OPEN shall assign, if currently available, each type of memory resources as described in the corresponding memory resource management data element. Memory resources shall be assigned according to the following rules:

- Assigning Minimum Memory to an Executable Load File (and its subsequent Application instance) shall not reduce the memory resources currently available on the card;

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0130

- Assigning Memory Quota to an Application shall not reduce the memory resources currently available on the card;
- The value of Memory Quota assigned to an Application shall not be less than the value of its Reserved Memory;
- Assigning Reserved Memory to an Executable Load File / Application shall reduce the memory resources currently available on the card at the time of its successful load / installation.

When memory resource management is supported, the OPEN shall manage available memory resources for each type of memory according to the following rules:

- At the time of the load's request (INSTALL [for load] command), the Minimum Memory requirements shall be currently available on the card;
- At the time of the successful load of an Executable Load File (last LOAD command), the amount of memory effectively allocated to that Executable Load File shall be charged against the Reserved Memory of that Executable Load File. If no Reserved Memory was assigned to that Executable Load File, the amount of memory shall reduce the memory resources currently available on the card;
- At the time of the installation of an Application (INSTALL [for install] command), the amount of memory effectively allocated to that Application shall first be charged against the Reserved Memory of that Application until it is entirely exhausted. When the Reserved Memory (if any) is exhausted, the amount of allocated memory shall be charged against that Application's Memory Quota and shall reduce the memory resources currently available on the card. When either the Memory Quota is exceeded or the memory resources currently available on the card are exhausted, the installation of the Application shall fail;
- During the lifetime of an Application, the amount of memory effectively allocated to the creation of data shall first be charged against the Reserved Memory of that Application, until it is entirely exhausted. When the Reserved Memory (if any) is exhausted, the amount of allocated memory shall be charged against that Application's Memory Quota and shall reduce the memory resources currently available on the card. When either the Memory Quota is exceeded or the memory resources currently available on the card are exhausted, the resource allocation shall fail;
- The successful removal of an Executable Load File / Application (DELETE command) shall augment the memory resources available on the card by the amount of memory effectively released and any unused part of the Reserved Memory (if any) of that Executable Load File / Application;
- The results of reporting memory resources are implementation dependent;
- The amount of memory effectively released by the deletion of data shall be reallocated to the Reserved Memory and Memory Quota assigned to that Application. If no Reserved Memory was assigned to that Application, the amount of released memory shall augment the memory resources available on the card.

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0131

# 10 Secure Communication

The GlobalPlatform documentation broadly defines the notion of secure communication over and above that defined in ISO standards. Specific mention is made of secure messaging for APDU commands; an optional authentication process is implied in most of the flow diagrams and Application access to Security Domain services implies that the ability to create a Secure Channel Session exists. This chapter defines the general rules that apply to all Secure Channel Protocols. Applications that utilize the services of Security Domains can use the Secure Channel Protocol supported by their associated Security Domains.

These protocols provide a means by which a Security Domain or an Application may communicate with an off-card entity within a logically secure environment.

Logical channels facilitate the possibility of more than one of the above off-card entities communicating concurrently with multiple Applications on the card, each within its own logically secure environment. It is the responsibility of the Security Domain provider to define whether this is possible or not.

## 10.1 Secure Channel

The Secure Channel provides a secure communication channel between a card and an off-card entity during an Application Session.

A Secure Channel Session is divided into three sequential phases:

- **Secure Channel Initiation** – when the on-card Application and the off-card entity have exchanged sufficient information enabling them to perform the required cryptographic functions. The Secure Channel Session initiation always includes the authentication of the off-card entity by the on-card Application;
- **Secure Channel Operation** – when the on-card Application and the off-card entity exchange data within the cryptographic protection of the Secure Channel Session. The Secure Channel services offered may vary from one Secure Channel Protocol to the other;
- **Secure Channel Termination** – when either the on-card Application or the off-card entity determines that no further communication is required or allowed via an established Secure Channel Session.

The 3 levels of security provided by the Secure Channel are defined in section 4.3.2 - *Secure Communication*.

A further level of security applies to sensitive data (e.g. secret keys) that shall always be transmitted as confidential data.

## 10.2 Explicit / Implicit Secure Channel

A Secure Channel Session is open after a successful initiation, including the authentication of the off-card entity by the on-card Application. A Secure Channel Session is terminated after the last successful communication within the same Secure Channel Session.

### 10.2.1 Explicit Secure Channel Initiation

Initiating a Secure Channel Session may be achieved by the off-card entity using appropriate APDU command(s) or by the on-card Application using the appropriate API. This method is the explicit Secure Channel creation. Appropriate APDU commands allow the off-card entity to instruct the card what level of

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0132

security is required for the current Secure Channel Session (integrity and/or confidentiality). They also give the off-card entity the possibility of selecting the keys to be used.

### 10.2.2 Implicit Secure Channel Initiation

The Secure Channel Session is initiated by the on-card Secure Channel Protocol handler, directly or through an API, when receiving the first APDU command that contains a cryptographic protection. The Secure Channel Protocol handler implicitly knows the required level of security. The Secure Channel Protocol handler may implicitly know which keys are to be used or may have been previously instructed by the off-card entity using appropriate APDU command(s) prior to initiating the Secure Channel Session.

### 10.2.3 Secure Channel Termination

Termination of the Secure Channel Session can be achieved by the on-card Application using the appropriate API or by the off-card entity using the appropriate APDU command.

Secure Channel termination causes all session data to be reset and all ICVs and session keys to be erased. The Current Security Level is set to NO_SECURITY and the Session Security Level is reset.

Termination of the Secure Channel Session occurs when one of the following conditions is met:

- The on-card Application Session is terminated - for instance when another Application is selected (i.e. the Application Session ends) on the same logical channel of the same card I/O interface. It may be the responsibility of the Application to initiate the termination of the Secure Channel Session when this occurs;
- The associated logical channel is explicitly closed;
- The card is reset (see ISO/IEC 7816-3 for contact cards), deactivated (see ISO/IEC 14443-3 for contactless cards) or powered off: i.e. the Card Session ends.

A Secure Channel Session is aborted but not terminated in the following cases:

- The on-card Application receives the first APDU command with an erroneous cryptographic protection;
- The on-card Application receives an APDU command without the required cryptographic protection set up during Secure Channel Session initiation;

If a Secure Channel Session is aborted, the Current Security Level is set to NO_SECURITY, the Session Security Level is not reset and the error condition persists until the Secure Channel Session is terminated.

A Secure Channel Session on a logical channel is never terminated in favor of a new Secure Channel Session being initiated on another logical channel.

## 10.3 Direct / Indirect Handling of a Secure Channel Protocol

There are two ways for the on-card Application to handle the Secure Channel Protocol.

- **Direct -** The Application owns its Secure Channel key set and fully implements the protocol: an example is Security Domains.
- **Indirect** – The Application uses the Security Domain services to handle the Secure Channel Protocol. This allows the Application using these services to be coded independently from the Secure Channel Protocol supported by the card.

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0133

## 10.4 Entity Authentication

Off-card entity authentication is achieved through the process of initiating a Secure Channel Session and provides assurance to the card that it is communicating with an authenticated entity. If any step in the authentication process fails, the process shall be restarted.

Authentication of the off-card entity is only provided for a limited time, a Secure Channel Session, and is valid only for the messages within that Secure Channel. This Secure Channel Session relates to the establishment and termination of a Secure Channel. If the Secure Channel Session is closed for any reason the off-card entity shall no longer be considered authenticated.

### 10.4.1 Authentication with Symmetric Cryptography

With a symmetric key Secure Channel Protocol (e.g. SCP01 or SCP02), an authenticated off-card entity is the entity which knows the secret Secure Channel keys needed to initiate a Secure Channel Session. The card cannot distinguish between the actual Application Provider of the Security Domain and one of its agents to whom a (set of) secret Secure Channel key(s) was provided. In this case, the card cannot distinguish between the Security Domain's provider and the provider of one of its associated Applications. Both are assumed to be the same entity: the Application Provider.

The Application is informed whether that unique entity, the Application Provider, has been successfully authenticated or not by examining the AUTHENTICATED indicator of the Current Security Level (see section 10.6 - *Security Levels*).

### 10.4.2 Authentication with Asymmetric Cryptography

With an asymmetric key Secure Channel Protocol (e.g. SCP10), any off-card entity that owns a pair of asymmetric keys and obtained a certificate for its public key certified by an authority recognized by the Security Domain can be successfully authenticated by that Security Domain. An authenticated off-card entity is the subject identified in the off-card entity's public key certificate verified during the Secure Channel Initiation. The card can distinguish between the actual Application Provider of the Security Domain and any other off-card entity using the off-card entity public key certificate's subject identifier.

In this case, the card can distinguish between the Security Domain's provider, the provider of one of its associated Applications, and any other off-card entity. The three are not necessarily the same entity: the Application Provider Id of each on-card entity is registered in the GlobalPlatform Registry at the time of the load or installation of that on-card entity and cannot be changed subsequently.

The Application is informed whether its own Application Provider has been authenticated by examining the AUTHENTICATED indicator of the Current Security Level (see section 10.6 - *Security Levels*). The ANY_AUTHENTICATED indicator of the Current Security Level indicates if another off-card entity, including the Security Domain's provider, has been authenticated or if the Application Provider Id is not registered. The Current Security Level viewed by the Target Application may differ from the Security Domain's view depending on the Secure Channel Protocol and the authenticated off-card entity's Application Provider Id (e.g. ANY_AUTHENTICATED for the Target Application and AUTHENTICATED for the Security Domain).

## 10.5 Secure Messaging

Secure messaging allows a sending entity to add confidentiality and/or integrity and authentication to the composition of an APDU message prior to the message being transmitted to a receiving entity:

- Integrity of an APDU command sent to the card or confidentiality of the command message and integrity of an APDU command sent to the card;

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0134

- Integrity of the sequence of APDU commands sent to the card within a Secure Channel Session;
- Optionally, depending on the Secure Channel Protocol, confidentiality and/or integrity of an APDU response message sent by the card, and integrity of the sequence of responses within a Secure Channel Session.

In the context of secure messaging, message integrity also provides data origin authentication.

## 10.6 Security Levels

A Secure Channel Protocol operates according to the Security Level that is established. This is done at two levels:

- A mandatory minimum Session Security Level is set at the initialization of the Secure Channel Session either explicitly or implicitly;
- A different Current Security Level may be set for an individual command or an individual response.

These Security Levels establish the minimum acceptable secure messaging protection that must be applied to protected messages, either for the whole session or for a specific command-response pair.

The following table shows the coding of Current Security Level:

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning |
|---|---|---|---|---|---|---|---|---|
| 1 | 0 | - | - | - | - | - | - | AUTHENTICATED |
| 0 | 1 | - | - | - | - | - | - | ANY_AUTHENTICATED |
| - | - | - | - | - | - | 1 | - | C_DECRYPTION |
| - | - | - | - | - | - | - | 1 | C_MAC |
| - | - | 1 | - | - | - | - | - | R_ENCRYPTION |
| - | - | - | 1 | - | - | - | - | R_MAC |
| - | - | - | - | X | X | - | - | RFU |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | NO_SECURITY_LEVEL |

**Table 10-1: Current Security Level**

Note that the Current Security Level cannot have its AUTHENTICATED and ANY_AUTHENTICATED indicators set simultaneously.

The rules for how Security Levels are handled are defined individually for Secure Channel Protocols '01', '02' and '10': see Appendices D, E and F for details.

## 10.7 Secure Channel Protocol Identifier

The Secure Channel Protocol identifies which particular secure communication protocol and set of security services are implemented in a Security Domain. The following values are assigned to the Secure Channel Protocol identifier:

- '**00**' – Not available
- '**01**' to '**7F**' - Reserved for use by GlobalPlatform
  - '**01**' – deprecated Secure Channel Protocol 1 defined in appendix D;
  - '**02**' – Secure Channel Protocol 2 defined in appendix E;

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0135

  - '**10**' - Secure Channel Protocol '10' defined in appendix F.

- '**80**' **to** '**EF**' – Reserved for use by individual schemes registered by GlobalPlatform
  - '**80**' - Secure Channel Protocol '80' defined in ETSI TS 102 225 and 102 226.
- '**F0**' **to** '**FF**' – Reserved for proprietary use and not registered by GlobalPlatform

The deprecated symmetric key Secure Channel Protocol '01' is backward compatible with the Open Platform Card Specification version 2.0.1'; it is deprecated in this version of the Specification.

The symmetric key Secure Channel Protocol '02' includes services in addition to those provided by Secure Channel Protocol '01' as well as optimizing the operation of some services compared to the deprecated Secure Channel Protocol '01'.

The Secure Channel Protocol '80' supports the Over The Air security scheme defined in ETSI TS 102 225.

The asymmetric key Secure Channel Protocol '10' offers authentication services using a Public Key Infrastructure (PKI) and secure messaging protection of commands and responses using symmetric cryptography.

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0136

# Part IV
# APDU
# Command
# Reference

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0137

# 11 APDU Command Reference

This chapter details the GlobalPlatform APDU commands that may be implemented. The commands are listed alphabetically.

The following table summarizes the APDU commands that shall be supported by a Security Domain with Authorized Management privilege, a Security Domain with Delegated Management privilege, a Security Domain with Final Application privilege and the requirements for support of these APDU commands by other Security Domains. When logical channels are supported, the MANAGE CHANNEL command is only processed by the OPEN and no Security Domain support is required for this command.

| Command | OP_READY | | | INITIALIZED | | | SECURED | | | CARD_LOCKED | | TERMINATED | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | AM SD | DM SD | SD | AM SD | DM SD | SD | AM SD | DM SD | SD | FA SD | SD | FA SD | SD |
| DELETE Executable Load File | | | | | | | | | | | | | |
| DELETE Executable Load File and related Application(s) | | | | | | | | | | | | | |
| DELETE Application | ✓ | | | ✓ | | | ✓ | | | | | | |
| DELETE Key | | | | | | | | | | | | | |
| GET DATA | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | |
| GET STATUS | ✓ | | | ✓ | | | ✓ | | | ✓ | | | |
| INSTALL [for load] | | | | | | | | | | | | | |
| INSTALL [for install] | | | | | | | | | | | | | |
| INSTALL [for load, install and make selectable] | | | | | | | | | | | | | |
| INSTALL [for install and make selectable] | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ | | | | | |
| INSTALL [for make selectable] | | | | | | | | | | | | | |
| INSTALL [for extradition] | | | | | | | | | | | | | |
| INSTALL [for registry update] | | | | | | | | | | | | | |

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0138

| Command | OP_READY | | | INITIALIZED | | | SECURED | | | CARD_LOCKED | | TERMINATED | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | AM SD | DM SD | SD | AM SD | DM SD | SD | AM SD | DM SD | SD | FA SD | SD | FA SD | SD |
| INSTALL [for personalization] | | | | | | | | | | | | | |
| LOAD | | | | | | | | | | | | | |
| PUT KEY | ✓ | | | ✓ | | | ✓ | | | | | | |
| SELECT | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | |
| SET STATUS | ✓ | | | ✓ | | | ✓ | | | ✓ | | | |
| STORE DATA | ✓ | | | ✓ | | | ✓ | | | | | | |

**Table 11-1: Authorized GlobalPlatform Commands per Card Life Cycle State**

Legend of Table 11-1:

AM SD: Security Domain with Authorized Management privilege.

DM SD: Security Domain with Delegated Management privilege.

FA SD: Security Domain with Final Application privilege. (Note: command support for an Application with Final Application Privilege which is not a Security Domain is subject to Issuer policy, within the constraints of what is permitted according to the card Life Cycle State.)

SD: Other Security Domain.

✓ : Support required.

Blank cell: Support optional.

Striped cell: Support prohibited.

Table 11-2 summarizes the minimum security requirements for the APDU commands.

| Command | Minimum Security |
|---|---|
| DELETE | Secure Channel initiation or digital signature verification |
| GET DATA | None |
| GET STATUS | Secure Channel initiation |
| INSTALL | Secure Channel initiation or digital signature verification |
| LOAD | Secure Channel initiation or digital signature verification |
| MANAGE CHANNEL | Not applicable |
| PUT KEY | Secure Channel initiation |
| SELECT | Not applicable |
| SET STATUS | Secure Channel initiation |
| STORE DATA | Secure Channel initiation |

**Table 11-2: Minimum Security Requirements for GlobalPlatform Commands**

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0139

## 11.1 General Coding Rules

The use of 'RFU' and '-' (dash) in tables in this chapter is as defined in Table 1-3: Abbreviations and Notations. If a bit is shown as RFU the bit should be set to zero by the off-card entity and the card shall ignore the value.

### 11.1.1 Life Cycle State Coding

The Executable Load File Life Cycle is coded on one byte as described in the following table:

| b8 | b7 | b6 | b5 | b4 | b3 | B2 | b1 | Meaning |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | LOADED |

**Table 11-3: Executable Load File Life Cycle Coding**

The Application Life Cycle has a bit-oriented coded value on one byte as described in the following table.

**Note:** the application has free use of bits b4-b7, and the coding of these bits is beyond the scope of this specification.

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | INSTALLED |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | SELECTABLE |
| 0 | X | X | X | X | 1 | 1 | 1 | Application Specific State |
| 1 | - | - | - | - | - | 1 | 1 | LOCKED |

**Table 11-4: Application Life Cycle Coding**

The Security Domain Life Cycle has a bit-oriented coded value on one byte as described in the following table:

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | INSTALLED |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | SELECTABLE |
| 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | PERSONALIZED |
| 1 | 0 | 0 | 0 | - | - | 1 | 1 | LOCKED |

**Table 11-5: Security Domain Life Cycle Coding**

The allowed Application and Security Domain Life Cycle transitions are described in chapter 5 - *Life Cycle Models*.

The Issuer Security Domain inherits the card Life Cycle State that has a bit-oriented coded value on one byte as described in the following table:

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | OP_READY |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | INITIALIZED |
| 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | SECURED |
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | CARD_LOCKED |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | TERMINATED |

**Table 11-6: Card Life Cycle Coding**

The allowed card Life Cycle transitions are described in chapter 5 - *Life Cycle Models*.

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0140

### 11.1.2 Privileges Coding

Privileges are coded on three bytes as described in Table 11-7, Table 11-8, and Table 11-9 (See section 6.6 - *Privileges* for additional details):

| 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 |

**Table 11-7: Privileges (byte 1)**

| 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 |

**Table 11-8: Privileges (byte 2)**

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning | Privilege Number |
|---|---|---|---|---|---|---|---|---|---|
| 1 | - | - | - | - | - | - | - | Receipt Generation | 16 |
| - | 1 | - | - | - | - | - | - | Ciphered Load File Data Block | 17 |
| - | - | 1 | - | - | - | - | - | Contactless Activation | 18 |
| - | - | - | 1 | - | - | - | - | Contactless Self-Activation | 19 |
| - | - | - | - | X | X | X | X | RFU | - |

**Table 11-9: Privileges (byte 3)**

### 11.1.3 General Error Conditions

The following table describes the error conditions that may be returned by any command:

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0141

| SW1 | SW2 | Meaning |
|---|---|---|
| '64' | '00' | No specific diagnosis |
| '67' | '00' | Wrong length in Lc |
| '68' | '81' | Logical channel not supported or is not active |
| '69' | '82' | Security status not satisfied |
| '69' | '85' | Conditions of use not satisfied |
| '6A' | '86' | Incorrect P1 P2 |
| '6D' | '00' | Invalid instruction |
| '6E' | '00' | Invalid class |

**Table 11-10: General Error Conditions**

## 11.1.4 Class Byte Coding

The class byte of all commands shall conform to ISO/IEC 7816-4 and shall be coded according to section 11.1.4.1 for commands addressed to the Basic Logical Channel and Supplementary Logical Channels 1, 2 and 3. For cards implementing four or more Supplementary Logical Channels the class byte of all commands addressed to Supplementary Logical Channel four to nineteen shall be coded according to section 11.1.4.2.

### 11.1.4.1 First Interindustry Class Byte Coding

The following table describes the first interindustry class byte coding:

| b8 | b7 | b6 | b5(*) | b4 | b3 | b2 | b1 | Meaning |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | - | - | - | - | Command defined in ISO/IEC 7816 |
| 1 | 0 | 0 | 0 | - | - | - | - | GlobalPlatform command |
| - | 0 | 0 | 0 | 0 | 0 | - | - | No secure messaging |
| - | 0 | 0 | 0 | 0 | 1 | - | - | Secure messaging - GlobalPlatform proprietary |
| - | 0 | 0 | 0 | 1 | 0 | - | - | Secure messaging - ISO/IEC 7816 standard, command header not processed (no C-MAC) |
| - | 0 | 0 | 0 | 1 | 1 | - | - | Secure messaging - ISO/IEC 7816 standard, command header authenticated (C-MAC) |
| - | 0 | 0 | 0 | - | - | X | X | Logical channel number |

**Table 11-11: CLA Byte Coding**

Class byte bits b1 and b2 may be set to define the required logical channel number according to ISO/IEC 7816;

- A class byte with bits b1 and b2 set to 00 indicates receipt of the command on the Basic Logical Channel;
- A class byte with bits b1 and b2 set to 01 (1), 10 (2) or 11 (3) indicates receipt of the command on a Supplementary Logical Channel.

Class byte bits b4 and b3 may be set to define the required secure messaging according to ISO/IEC 7816-4:

- A class byte with bits b4 and b3 set to 00 indicates no secure messaging;

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0142

- A class byte with bits b4 and b3 set to 01 indicates secure messaging with GlobalPlatform format;
- A class byte with bits b4 and b3 set to 11 or 10 indicates secure messaging with ISO/IEC 7816-4 format.

(*) Note: class byte bit b5 is always 0 except if it is coded for command chaining as defined in appendix F.

#### 11.1.4.2 Further Interindustry Class Byte Coding

The following table describes the further interindustry class byte coding.

| b8 | b7 | b6 | b5(*) | b4 | b3 | b2 | b1 | Meaning |
|---|---|---|---|---|---|---|---|---|
| 0 | 1 | - | 0 | - | - | - | - | Command defined in ISO/IEC 7816 |
| 1 | 1 | - | 0 | - | - | - | - | GlobalPlatform command |
| - | 1 | 0 | 0 | - | - | - | - | No secure messaging |
| - | 1 | 1 | 0 | - | - | - | - | Secure messaging - ISO/IEC 7816 or GlobalPlatform proprietary |
| - | 1 | - | 0 | X | X | X | X | Logical channel number |

**Table 11-12: CLA Byte Coding**

Class byte bits b1 to b4 may be set to define the required logical channel number according to ISO/IEC 7816;

- A class byte with bit b7 set to 1 indicates in bits b4 to b1 (values 0000 to 1111) receipt of the command on Supplementary Logical Channel 4 to 19.

Class byte bit b6 may be set to define the required secure messaging according to ISO/IEC 7816-4 or proprietary GlobalPlatform format:

- A class byte with bit b6 set to 0 indicates no secure messaging;
- A class byte with bit b6 set to 1 indicates secure messaging with GlobalPlatform format or with ISO/IEC 7816-4 format.

### 11.1.5 APDU Message and Data Length

All GlobalPlatform APDU messages and data elements are counted in bytes. All GlobalPlatform commands comply with ISO/IEC 7816 short message lengths i.e. Lc and Le bytes coded on one byte.

All GlobalPlatform command messages (including the APDU header) are limited to 255 bytes in length. All GlobalPlatform commands that expect response data have their Le byte set to zero, indicating that all available response data shall be returned. According to ISO/IEC 7816-4, all GlobalPlatform responses returned in APDU response messages shall have a maximum length of 256 bytes of response data.

All length fields of GlobalPlatform messages and data objects defined in this specification, except for Lc and Le, are coded as defined for ASN.1 BER-TLV (see ISO 8825-1): 1 byte for a length up to 127, 2 bytes for a length up to 255, and 3 bytes for a length up to 65535, except where otherwise stated.

This version of the Specification is written as though most command functions can be handled with a single APDU command and response pair. This is done in order to simplify the description, and is not intended to preclude the use of multiple commands being used where such a mechanism is provided, as indicated for each command: such as (for GlobalPlatform commands) the 'more commands' bit in the P1 byte and status bytes controlling the return of additional data; and (for ISO commands) command and response chaining.

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0143

### 11.1.6 Confirmations in Response Messages

The confirmation shall be structured according to the following table:

| Length | Data Element | Presence |
|---|---|---|
| 1-2 | Length of Receipt ('00' - '7F' or '81 80' - '81 FF') | Mandatory |
| 0-n | Receipt | Conditional |
| 5-n | Confirmation Data | Mandatory |

**Table 11-13: Confirmation Structure**

The length field for the Receipt is coded according to ASN.1 BER-TLV (see ISO 8825-1).

Confirmation Data is structured according to the following table:

| Length | Data Element | Presence |
|---|---|---|
| 1 | Length of Confirmation Counter | Mandatory |
| 2 | Confirmation Counter | Mandatory |
| 1 | Length of Card Unique Data | Mandatory |
| 1-n | SD Unique Data | Mandatory |
| 1 | Length of Token identifier | Conditional |
| 0-n | Token identifier | Conditional |
| 1 | Length of Token Data digest | Optional |
| 0-n | Token Data digest | Optional |

**Table 11-14: Confirmation Data**

The presence of Token identifier depends on whether a Token identifier was included in the original Token. The presence of the Token Data digest is dependent on the policy of the Security Domain with Receipt Generation privilege.

Security Domain unique data is the concatenation without delimiters of the Security Domain Provider Identification Number ('42') and the Security Domain Image Number (SDIN, tag '45') of the Security Domain generating the confirmation (with the Receipt Generation Privilege).

### 11.1.7 Implicit Selection Parameter Coding

The Implicit Selection parameter (tag 'CF') indicates that this Application is to be implicitly selected on one (or more) specific card interface(s) for a specific logical channel, see section 6.6.3 - *Privilege Management*. Setting both bits 8 and 7 to zero indicates that this Application is to be selectable only explicitly with a SELECT [by name] command and the logical channel number shall be ignored by the card. The value field is coded on one byte as follows:

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning |
|---|---|---|---|---|---|---|---|---|
| 1 | - | - | - | - | - | - | - | Contactless I/O |
| - | 1 | - | - | - | - | - | - | Contact I/O |
| - | - | X | - | - | - | - | - | RFU |
| - | - | - | X | X | X | X | X | Logical channel number (0 to 19) |

**Table 11-15: Implicit Selection Parameter**

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0144

### 11.1.8 Key Type Coding

Key type may be coded on one or two bytes. When coded on two bytes, the first byte shall be set to 'FF' to indicate an extended format of the key data field. The second or only byte shall be coded according to the following table:

| Value | Meaning |
|---|---|
| '00'-'7F' | Reserved for private use |
| '80' | DES – mode (ECB/CBC) implicitly known |
| '81' | Reserved (Triple DES) |
| '82' | Triple DES in CBC mode |
| '83' | DES in ECB mode |
| '84' | DES in CBC mode |
| '85' | Pre-Shared Key for Transport Layer Security |
| '86'-'87' | RFU (symmetric algorithms) |
| '88' | AES (16, 24, or 32 long keys) |
| '89'-'8F' | RFU (symmetric algorithms) |
| '90' | HMAC-SHA1 – length of HMAC is implicitly known |
| '91' | HMAC-SHA1-160 – length of HMAC is 160 bits |
| '92'-'9F' | RFU (symmetric algorithms) |
| 'A0' | RSA Public Key - public exponent e component (clear text) |
| 'A1' | RSA Public Key - modulus N component (clear text) |
| 'A2' | RSA Private Key - modulus N component |
| 'A3' | RSA Private Key - private exponent d component |
| 'A4' | RSA Private Key - Chinese Remainder P component |
| 'A5' | RSA Private Key - Chinese Remainder Q component |
| 'A6' | RSA Private Key - Chinese Remainder PQ component ( $q^{-1}$ mod p ) |
| 'A7' | RSA Private Key - Chinese Remainder DP1 component ( d mod (p-1) ) |
| 'A8' | RSA Private Key - Chinese Remainder DQ1 component ( d mod (q-1) ) |
| 'A9'-'FE' | RFU (asymmetric algorithms) |
| 'FF' | Extended format |

**Table 11-16: Key Type Coding**

### 11.1.9 Key Usage Qualifier Coding

The values for the Key usage qualifier parameter are set according to the following table:

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning |
|---|---|---|---|---|---|---|---|---|
| 1 | - | - | - | - | - | - | - | Verification (DST, CCT, CAT), Encipherment (CT) |
| - | 1 | - | - | - | - | - | - | Computation (DST, CCT, CAT), Decipherment (CT) |
| - | - | 1 | - | - | - | - | - | Secure messaging in response data fields (CT, CCT) |

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0145

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning |
|---|---|---|---|---|---|---|---|---|
| - | - | - | 1 | - | - | - | - | Secure messaging in command data fields (CT, CCT) |
| - | - | - | - | 1 | - | - | - | Confidentiality (CT) |
| - | - | - | - | - | 1 | - | - | Cryptographic Checksum (CCT) |
| - | - | - | - | | - | 1 | - | Digital Signature (DST) |
| - | - | - | - | - | - | - | 1 | Cryptographic Authorization (CAT) |

**Table 11-17: Key Usage Qualifier**

The following values are used by GlobalPlatform. Values are independent of the cryptographic algorithm used.

- C-MAC = '14', R-MAC = '24', C-MAC + R-MAC = '34';
- C-ENC = '18', R-ENC = '28', C-ENC + R-ENC = '38';
- C-DEK = '48', R-DEK = '88', C-DEK + R-DEK = 'C8';
- PK_SD_AUT = '82';
- SK_SD_AUT = '42';
- Token = '81';
- Receipt = '44';
- DAP = '84';
- PK_SD_AUT + Token = '83';
- SK_SD_AUT + Receipt = '43';
- PK_SD_AUT + DAP = '86';
- PK_SD_AUT + Token + DAP = '87'.

### 11.1.10 Key Access Coding

The values for the Key Access parameter are set according to the following table (see appendix 7.5.2 - *Key Access Conditions* for details):

| Value | Description |
|---|---|
| '00' | The key may be used by the Security Domain and any associated Application |
| '01' | The key may only be used by the Security Domain |
| '02' | The key may be used by any Application associated with the Security Domain but not by the Security Domain itself |
| '03'- '1F' | RFU |
| '20'- 'FE' | Proprietary usage |
| 'FF' | Not available |

**Table 11-18: Key Access**

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0146

### 11.1.11 Tag Coding

All tags of GlobalPlatform data objects are coded as defined by ASN.1 BER-TLV rules (see ISO 8825-1).

For Security Domain data objects present in GlobalPlatform APDU messages, BER-TLV tags are coded according to the following rules:

- '00' to '7E' – Reserved for use by ISO/IEC;
- '80' to '9E' and 'A0' to 'BE' – Reserved for use depending on the context (see note);
- 'C0' to 'DD' and 'E0' to 'FD' – Reserved for use by GlobalPlatform or individual schemes registered by GlobalPlatform;
  - 'CA' and 'EA' – Reserved for use by ETSI TS 102 226 specification;
- 'DE' and 'FE' – Reserved for proprietary use and not registered by GlobalPlatform;
- '1F 1F' to '7F 7F' – Reserved for use by ISO/IEC;
- '9F 1F' to '9F 7F' and 'BF 1F' to 'BF 7F' – Reserved for use depending on the context (see note);
- 'DF 1F' to 'DF 7F' and 'FF 1F' to 'FF 7F' – Reserved for use by GlobalPlatform or individual schemes registered by GlobalPlatform;
  - 'FF 1F' to 'FF 3F' – Reserved for use by ETSI TS 102 226 specification.

Note: Context dependent tags are assigned by the authority defining the context, e.g. ISO/IEC for data objects embedded in other ISO/IEC data objects or GlobalPlatform for data objects embedded in other GlobalPlatform data objects.

Tag allocation for any data objects embedded in the constructed tag 'FE' (reserved for proprietary use) is beyond the scope of this specification. Applying BER-TLV rules in this case is recommended.

### 11.1.12 Data Grouping Identifier (DGI) Coding

The DGI shall be coded on two byes in binary format, followed by a length indicator coded as defined in GP Systems Scripting Language Specification v1.1.0, annex B.

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0147

## 11.2 DELETE Command

### 11.2.1 Definition and Scope

The DELETE command is used to delete a uniquely identifiable object such as an Executable Load File, an Application, an Executable Load File and its related Applications or a key. In order to delete an object, the object shall be uniquely identifiable by the selected Application.

### 11.2.2 Command Message

The DELETE command message is coded according to the following table:

| Code | Value | Meaning |
|---|---|---|
| CLA | '80' - '8F',<br>'C0' - 'CF' or<br>'E0' - 'EF' | See section 11.1.4 |
| INS | 'E4' | DELETE |
| P1 | 'xx' | Reference control parameter P1 |
| P2 | 'xx' | Reference control parameter P2 |
| Lc | 'xx' | Length of data field |
| Data | 'xxxx…' | TLV coded objects (and MAC if present) |
| Le | '00' | |

**Table 11-19: DELETE Command Message**

#### 11.2.2.1 Reference Control Parameter P1

Reference control parameter P1 allows for command data to be longer than 255 bytes and to be segmented into components of arbitrary size and transmitted in a series of DELETE commands. P1 indicates whether the command data is one of a sequence of components or the last (or only) component.

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning |
|---|---|---|---|---|---|---|---|---|
| 0 | - | - | - | - | - | - | - | Last (or only) command |
| 1 | - | - | - | - | - | - | - | More DELETE commands |
| - | X | X | X | X | X | X | X | RFU |

**Table 11-20: DELETE Reference Control Parameter P1**

#### 11.2.2.2 Reference Control Parameter P2

The reference control parameter P2 indicates whether the object in the data field is being deleted or whether the object in the data field and its related objects are being deleted. It shall be coded according to the following table:

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning |
|---|---|---|---|---|---|---|---|---|
| 0 | - | - | - | - | - | - | - | Delete object |
| 1 | - | - | - | - | - | - | - | Delete object and related object |

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0148

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning |
|---|---|---|---|---|---|---|---|---|
| - | X | X | X | X | X | X | X | RFU |

**Table 11-21: DELETE Reference Control Parameter P2**

#### 11.2.2.3 Data Field Sent in the Command Message

The data field of the DELETE command message shall contain the TLV coded name(s) of the object to be deleted.

##### 11.2.2.3.1 Delete [card content] Data Field

The Application or Executable Load File AID may be followed by a Control Reference Template for Digital Signature and a Delete Token, as follows:

| Tag | Length | Name | Presence |
|---|---|---|---|
| '4F' | 5-16 | Executable Load File or Application AID | Mandatory |
| 'B6' | Variable | Control Reference Template for Digital Signature | Conditional |
| '42' | 1-n | Identification Number of the Security Domain with the Token Verification privilege | Optional |
| '45' | 1-n | Image number of the Security Domain with the Token Verification privilege | Optional |
| '5F20' | 1-n | Application Provider identifier | Optional |
| '93' | 1-n | Token identifier/number (digital signature counter) | Conditional |
| '9E' | 1-n | Delete Token | Conditional |

**Table 11-22: Delete [card content] Command Data Field**

The identity of the Application or Executable Load File to delete shall be specified using the tag for an AID ('4F') followed by a length and the AID of the Application or Executable Load File. When simultaneously deleting an Executable Load File and all its related Applications, only the identity of the Executable Load File shall be provided.

The presence of the Control Reference Template for Digital Signature and Delete Token depends on the Card Issuer's policy. The presence of the data objects in tag 'B6' and the sub-tags ‘42’, ‘45’, ‘5F20’ and ‘93’ are strongly recommended when using SCP10.

The length fields for the Control Reference Template for Digital Signature and the Delete Token are coded according to ASN.1 BER-TLV (see ISO 8825-1).

##### 11.2.2.3.2 Delete (Key) Data Field

To delete one or more keys, the Key Version Number and/or the Key Identifier are included in the command data field as follows:

| Tag | Length | Meaning | Presence |
|---|---|---|---|
| 'D0' | 1 | Key Identifier | Conditional |
| 'D2' | 1 | Key Version Number | Conditional |

**Table 11-23: DELETE [key] Command Data Field**

A single key is deleted when both the Key Identifier ('D0') and the Key Version Number ('D2') are provided in the DELETE command message data field. Multiple keys may be deleted if one of these values is

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0149

omitted (i.e. all keys with the specified Key Identifier or Key Version Number). The options available for omitting these values are conditional on the Issuer's policy.

### 11.2.3 Response Message

A data field shall always be returned in the response message. The content of the data field is only relevant in the case of Delegated Management i.e. if a Security Domain with the Delegated Management privilege is deleting an Application or Executable Load File, a Receipt may be present in the data field depending on the security policy of the Card Issuer.

#### 11.2.3.1 Data Field Returned in the Response Message

For a DELETE [key] command, a single byte of '00' shall be returned indicating that no additional data is present.

For a DELETE [card content] command being issued to a Security Domain with the Delegated Management privilege, the data field may contain the confirmation of the delete procedure. The overall length of the response message shall not exceed 256 bytes.

The following table describes the structure of the DELETE response data field. The length field for the Delete Confirmation is coded according to ASN.1 BER-TLV (see ISO 8825-1).

| Name | Length | Value | Presence |
|---|---|---|---|
| Length of delete confirmation | 1-2 | '00' - '7F' or '81 80' - '81 FF' | Mandatory |
| Delete confirmation | 0-n | 'xxxx...' - see section 11.1.6 | Conditional |

**Table 11-24: DELETE Response Data Field**

#### 11.2.3.2 Processing State Returned in the Response Message

A successful execution of the command shall be indicated by status bytes '90' '00'.

This command may either return a general error condition as listed in section 11.1.3 - *General Error Conditions* or one of the following error conditions.

| SW1 | SW2 | Meaning |
|---|---|---|
| '65' | '81' | Memory failure |
| '6A' | '88' | Referenced data not found |
| '6A' | '82' | Application not found |
| '6A' | '80' | Incorrect values in command data |

**Table 11-25: DELETE Error Conditions**

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0150

# 11.3 GET DATA Command

## 11.3.1 Definition and Scope

The GET DATA command is used to retrieve either a single data object, which may be constructed, or a set of data objects. Reference control parameters P1 and P2 coding is used to define the specific data object tag. The data object may contain information pertaining to a key.

## 11.3.2 Command Message

The GET DATA command message is coded according to the following table:

| Code | Value | Meaning |
|---|---|---|
| CLA | '00' - '0F',<br>'40' - '4F',<br>'60' - '6F',<br>'80' - '8F',<br>'C0' - 'CF' or<br>'E0' - 'EF' | See section 11.1.4 |
| INS | 'CA' or 'CB' | GET DATA<br>- If CLA = '00' - '0F', '40' - '4F', '60' - '6F', even or odd instruction code 'CA' or 'CB';<br>- If CLA = '80' - '8F', 'C0' - 'CF' or 'E0' - 'EF', even instruction code 'CA'. |
| P1 | 'xx' | '00' or high order tag value |
| P2 | 'xx' | Low order tag value |
| Lc | 'xx' | Not present if no command data, or length of data field. |
| Data | 'xxxx…' | Tag list and/or MAC if present. |
| Le | '00' | |

**Table 11-26: GET DATA Command Message**

According to ISO/IEC 7816-4, the odd instruction code ‘CB’ in conjunction with a class byte indicating an ISO command (CLA set to '00' - '0F', '40' - '4F' or '60' - '6F') is used to retrieve the contents of a file. It may be used to retrieve the list of Applications on the card (P1-P2 set to ‘2F 00’).

### 11.3.2.1 Parameter P1 and P2

Parameters P1 and P2 define the tag of the data object to be read.

The value '2F 00' indicates a request to obtain details of Applications on the card, as defined in ISO/IEC 7816-4. The instruction code shall be set to 'CA' if the class byte indicates a GlobalPlatform command (CLA set to '80' - '8F', 'C0' - 'CF' or 'E0' - 'EF') or 'CB' if the class byte indicates an ISO command (CLA set to '00' - '0F', '40' - '4F' or '60' - '6F').

Security Domains shall support at least the following data object tags:

- Tag '42': Issuer Identification Number (or Security Domain Provider Identification Number);
- Tag '45': Card Image Number (or Security Domain Image Number);

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0151

- Tag '66': Card Data (or Security Domain Management Data);
- Tag 'E0': Key Information Template.

A Security Domain may support the following data object tags:

- Tag 'D3': Current Security Level;
- Tag '2F00': List of Applications belonging to the Security Domain, or every application on the card if the Security Domain has Global Registry Privilege;
- Tag 'FF21': Extended Card Resources Information available for Card Content Management, as defined in ETSI TS 102 226.

If present, the Security Domain with Receipt Generation privilege shall support the following additional data object tag:

- Tag 'C2': Confirmation Counter.

A Security Domain supporting Secure Channel Protocol '02' shall support the following data object tag:

- Tag 'C1': Sequence Counter of the default Key Version Number.

For a Security Domain supporting only Secure Channel Protocol '01', an attempt to retrieve the Sequence Counter of the default Key Version Number (tag 'C1') shall be rejected.

Other tags as defined in section 11.1.11 - *Tag Coding* may be available for data objects supported by a Security Domain.

#### 11.3.2.2 Data Field Sent in the Command Message

The data field of the GET DATA command message shall be empty unless a tag list and/or a MAC is required. For retrieving a list of applications present on the card (P1-P2 set to '2F 00') a tag list shall be present and coded as '5C 00'.

### 11.3.3 Response Message

#### 11.3.3.1 Data Field Returned in the Response Message

When the class byte indicates a GlobalPlatform proprietary command (bit b8 = 1), the GET DATA response data field shall contain the TLV coded data object referred to in reference control parameters P1 and P2 of the command message, except where P1-P2 are set to '2F 00'.

Where the class byte indicates an ISO command (bit b8 = 0), the GET DATA response data field shall contain only the value of the TLV coded data object referred to in reference control parameters P1 and P2 of the command message, except where P1-P2 are set to '2F 00'.

When retrieving key information for the currently selected Application, the key information is returned in the template 'E0' where each Key Information Data data object is introduced by the tag 'C0'. Its structure depends on the value of Key Type. If the Key Type is coded on one byte (value other than 'FF'), the Key Information Data is structured as follows:

| Name | Length | Value | Presence |
|---|---|---|---|
| Key Identifier | 1 | Key Identifier value | Mandatory |
| Key Version Number | 1 | Key Version Number value | Mandatory |
| Key type of first (or only) key component | 1 | '00' - 'FE', See section 11.1.8 - *Key Type Coding* | Mandatory |

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0152

| Name | Length | Value | Presence |
|---|---|---|---|
| Length of first (or only) key component | 1 | '01' - 'FF' | Mandatory |
| … | … | … | |
| Key type of last key component | 1 | '00' - 'FE', See section 11.1.8 - *Key Type Coding* | Conditional |
| Length of last key component | 1 | '01' - 'FF' | Conditional |

**Table 11-27: Key Information Data Structure - Basic**

If the Key Type is coded on two bytes (first byte = 'FF'), the Key Information Data is structured as follows:

| Name | Length | Value | Presence |
|---|---|---|---|
| Key Identifier | 1 | Key Identifier value | Mandatory |
| Key Version Number | 1 | Key Version Number value | Mandatory |
| Key type of first (or only) key component | 2 | 'FF xx' - see section 11.1.8 - *Key Type Coding* | Mandatory |
| Length of first (or only) key component | 2 | '00 01' - '7F FF' | Mandatory |
| … | … | … | |
| Key type of last key component (if any) | 2 | 'FF xx' - See section 11.1.8 - *Key Type Coding* | Conditional |
| Length of last key component (if any) | 2 | '00 01' - '7F FF' | Conditional |
| Length of Key Usage | 1 | '00' - '01' | Mandatory |
| Key usage | 0 or 1 | 'xx' - See section 11.1.9 | Conditional |
| Length of Key Access | 1 | '00' - '01' | Mandatory |
| Key Access | 0 or 1 | 'xx' - See section 11.1.10 | Conditional |

**Table 11-28: Key Information Data Structure - Extended**

The presence of Key Usage and Key Access is conditional on the data having been supplied when the key was loaded on the card.

When retrieving Extended Card Resources Information with tag 'FF21', the response shall be coded as defined in ETSI TS 102 226.

When retrieving the list of Applications present on the card, the response shall be coded as a series of Application Template data objects (tag '61') as defined in ISO/IEC 7816-4. An example of the response is as follows:

| Tag | Length | Name | Presence |
|---|---|---|---|
| '61' | 7-n | Application Template | Mandatory |
| '4F' | 5-16 | Application AID | Mandatory |
| | ... | ... | |
| '61' | 7-n | Application Template | Mandatory |
| '4F' | 5-16 | Application AID | Mandatory |
| | ... | ... | |

**Table 11-29: List of On-Card Applications**

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0153

#### 11.3.3.2 Processing State Returned in the Response Message

A successful execution of the command shall be indicated by status bytes '90' '00'.

This command may either return a general error condition as listed in section 11.1.3 - *General Error Conditions* or the following error condition.

| SW1 | SW2 | Meaning |
|---|---|---|
| '6A' | '88' | Referenced data not found |

**Table 11-30: GET DATA Error Conditions**

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0154

# 11.4 GET STATUS Command

## 11.4.1 Definition and Scope

The GET STATUS command is used to retrieve Issuer Security Domain, Executable Load File, Executable Module, Application or Security Domain Life Cycle status information according to a given match/search criteria.

## 11.4.2 Command Message

The GET STATUS command message shall be coded according to the following table.

| Code | Value | Meaning |
|---|---|---|
| CLA | '80' - '8F',<br>'C0' - 'CF' or<br>'E0' - 'EF' | See section 11.1.4 |
| INS | 'F2' | GET STATUS |
| P1 | 'xx' | Reference control parameter P1 |
| P2 | 'xx' | Reference control parameter P2 |
| Lc | 'xx' | Length of data field |
| Data | 'xx...' | Search criteria (and MAC if present) |
| Le | '00' | |

**Table 11-31: GET STATUS Command Message**

### 11.4.2.1 Reference Control Parameter P1

Reference control parameter P1 is used to select a subset of statuses to be included in the response message. It is coded as follows:

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning |
|---|---|---|---|---|---|---|---|---|
| 1 | - | - | - | - | - | - | - | Issuer Security Domain |
| - | 1 | - | - | - | - | - | - | Applications, including Security Domains |
| - | - | 1 | - | - | - | - | - | Executable Load Files |
| - | - | - | 1 | - | - | - | - | Executable Load Files and Executable Modules |
| - | - | - | - | X | X | X | X | RFU |

**Table 11-32: GET STATUS Reference Control Parameter P1**

The following values of the reference control parameter shall be supported:

**'80'** – Issuer Security Domain only. In this case the search criteria is ignored and the Issuer Security Domain information is returned.

**'40'** – Applications and Supplementary Security Domains only.

**'20'** – Executable Load Files only.

**'10'** – Executable Load Files and their Executable Modules only.

The ability to differentiate a Security Domain from an Application is achieved through privileges.

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0155

#### 11.4.2.2 Reference Control Parameter P2

The reference control parameter P2 controls the number of consecutive GET STATUS command and indicates the format of the response message. It shall be coded according to the following table.

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning |
|---|---|---|---|---|---|---|---|---|
| X | X | X | X | X | X | - | - | RFU |
| - | - | - | - | - | - | - | 0 | Get first or all occurrence(s) |
| - | - | - | - | - | - | - | 1 | Get next occurrence(s) |
| - | - | - | - | - | - | 0 | - | Deprecated: response data structure according to Table 11-35 and Table 11-37 |
| - | - | - | - | - | - | 1 | - | Response data structure according to Table 11-36 |

**Table 11-33: GET STATUS Reference Control Parameter P2**

A GET STATUS [get next occurrence] command shall be rejected if no prior GET STATUS [get first or all occurrence(s)] was received within the current Application Session.

When retrieving the status of the Issuer Security Domain only, the get next occurrence indicator shall be rejected.

Requesting a response coded according to Table 11-36 is recommended when interrogating a card compliant to this version of the specification or Amendment A of version 2.1.1. Note that cards compliant to previous versions of this specification may only support response data structures as defined in Table 11-35 and Table 11-37.

#### 11.4.2.3 Data Field Sent in the Command Message

The data field is structured as follows:

| Tag | Length | Name | Presence |
|---|---|---|---|
| '4F' | 0-16 | Application AID | Mandatory |
| 'xx' or 'xxxx' | 0-n | Other search criteria | Optional |
| ... | ... | ... | ... |
| '5C' | 1-n | Tag list | Optional |

**Table 11-34: GET STATUS Command Data Field**

The GET STATUS command message data field shall contain at least one TLV coded search qualifier: the AID (tag '4F'). It shall be possible to search for all the occurrences that match the selection criteria according to the reference control parameter P1 using a search criteria of '4F' '00'.

It shall be possible to search for all occurrences with the same RID.

Other search criteria may be added. In such cases, the additional search criteria shall be TLV coded and appended after the mandatory search criterion AID (tag '4F'). When not supported by the card, additional search criteria shall be ignored.

The search is limited to the Executable Load Files, Applications and Security Domains that are directly or indirectly associated with the on-card entity receiving the command. When the on-card entity receiving the command has the Global Registry privilege, the search applies to all Executable Load Files, Applications and Security Domains registered in the GlobalPlatform Registry.

The tag list (tag '5C') indicates to the card how to construct the response data for each on-card entity matching the search criteria. Its value field contains a concatenation of tags (without delimitation) indicating the data objects to include in the response. If an on-card entity that matches the search criteria

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0156

is found in GlobalPlatform Registry without the corresponding data object, an error status shall be returned. The tag list may only be present when reference control parameter P2 indicates a TLV-coded response (i.e. bit b2 of P2 set to 1). When not supported by the card, the tag list shall be ignored.

## 11.4.3 Response Message

### 11.4.3.1 Data Field Returned in the Response Message

Based upon the search criteria of the GET STATUS command data field and the selection criteria of reference control parameter P1 and P2, multiple occurrences of the data structure in the following tables may be returned. Responses coded according to Table 11-35 and Table 11-37 are deprecated. It is therefore recommended to use the encoding according to Table 11-36.

| Name | Length | Value | Presence |
|---|---|---|---|
| Length of Application AID | 1 | '05' - '10' | Mandatory |
| Application AID | 5-16 | 'xxxx...' | Mandatory |
| Life Cycle State | 1 | 'xx' - see section 11.1.1 | Mandatory |
| Privileges (byte 1) | 1 | 'xx' - see section 11.1.2 | Mandatory |

**Table 11-35: Issuer Security Domain, Application and Executable Load File Information Data**

Note: For backward compatibility, when the deprecated encoding is used and the Privileges are received coded on one byte, the off-card entity should assume that the second and third bytes are set to the default values as defined in section 6.6.2.

| Tag | Length | Name |
|---|---|---|
| 'E3' | Variable | GlobalPlatform Registry related data |
| '4F' | 5-16 | AID |
| '9F70' | 1 | Life Cycle State |
| 'C5' | 0,1,3 | Privileges (byte 1 - byte 2 – byte 3) see section 11.1.2 |
| 'CF' | 1 | First Implicit Selection Parameter, see section 11.1.7 |
| … | … | … |
| 'CF' | 1 | Last Implicit Selection Parameter, see section 11.1.7 |
| 'C4' | 1-n | Application's Executable Load File AID |
| 'CE' | 1-n | Executable Load File Version Number |
| '84' | 1-n | First Executable Module AID |
| … | ... | … |
| '84' | 1-n | Last Executable Module AID |
| 'CC' | 1-n | Associated Security Domain's AID |

**Table 11-36: GlobalPlatform Registry Data (TLV)**

If tag lists are supported by the card, the response shall be coded according to Table 11-36 and shall only contain the data objects whose tags are listed in the tag list (tag '5C') of the command, the order of the

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0157

data objects within the GlobalPlatform Registry data (template ‘E3’) being arbitrary. If no tag list (tag ‘5C’) is present in the command or if the card does not support tag lists, a response coded according to Table 11-36 shall contain the following data objects:

- The AID (tag ‘4F’) and Life Cycle State (tag ‘9F70’) shall be present;
- Privileges (tag ‘C5’) shall be present for the Issuer Security Domain, Supplementary Security Domains and Applications and shall be absent for Executable Load Files;
- The Executable Modules (tag ‘84’) shall be present if reference control parameter P1 indicates Executable Load Files and their Executable Modules only (bit b5 of P1 set to 1) and if the Runtime Environment supports Executable Modules. Tag '84' is not present for an Executable Load File that does not contain any Executable Modules.

Note: the Executable Load File Version Number format and contents are beyond the scope of this specification. It shall consist of the version information contained in the original Load File: on a Java Card based card, this version number represents the major and minor version attributes of the original Load File Data Block.

| Name | Length | Value | Presence |
|---|---|---|---|
| Length of Executable Load File AID | 1 | '05' - '10' | Mandatory |
| Executable Load File AID | 5-16 | 'xxxx…' | Mandatory |
| Executable Load File Life Cycle State | 1 | 'xx' - see section 11.1.1 | Mandatory |
| Privileges | 1 | '00' | Mandatory |
| Number of Executable Modules | 1 | '00' - '7F' | Mandatory |
| Length of Executable Module AID | 1 | '05' - '10' | Conditional |
| Executable Module AID | 5-16 | 'xxxx…' | Conditional |
| … | … | … | ... |
| Length of Executable Module AID | 1 | '05' - '10' | Conditional |
| Executable Module AID | 5-16 | 'xxxx…' | Conditional |

**Table 11-37: Executable Load File and Executable Module Information Data**

The Executable Modules shall be present if reference control parameter P1 indicates Executable Load Files and their Executable Modules only (bit b5 of P1 set to 1) and if the Runtime Environment supports Executable Modules.

#### 11.4.3.2 Processing State Returned in the Response Message

A successful execution of the command shall be indicated by status bytes '90' '00'.

The command may return the following warning condition:

| SW1 | SW2 | Meaning |
|---|---|---|
| '63' | '10' | More data available |

**Table 11-38: GET STATUS Warning Condition**

Following status '63 10' a subsequent GET STATUS [get next occurrence(s)] may be issued to retrieve additional data.

This command may return a general error condition as listed in section 11.1.3 - *General Error Conditions* or one of the following error conditions.

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0158

| SW1 | SW2 | Meaning |
|---|---|---|
| '6A' | '88' | Referenced data not found |
| '6A' | '80' | Incorrect values in command data |

**Table 11-39: GET STATUS Error Conditions**

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0159

# 11.5 INSTALL Command

## 11.5.1 Definition and Scope

The INSTALL command is issued to a Security Domain to initiate or perform the various steps required for Card Content management.

## 11.5.2 Command Message

The INSTALL command message shall be coded according to the following table.

| Code | Value | Meaning |
|---|---|---|
| CLA | '80' - '8F',<br>'C0' - 'CF' or<br>'E0' - 'EF' | See section 11.1.4 |
| INS | 'E6' | INSTALL |
| P1 | 'xx' | Reference control parameter P1 |
| P2 | '00', '01' or '03' | Reference control parameter P2 |
| Lc | 'xx' | Length of data field |
| Data | 'xxxx…' | Install data (and MAC if present) |
| Le | '00' | |

**Table 11-40: INSTALL Command Message**

### 11.5.2.1 Reference Control Parameter P1

The reference control parameter P1 of the INSTALL command defines the specific role of the INSTALL command and also allows for command data to be longer than 255 bytes and to be segmented into arbitrary components and transmitted in a series of INSTALL commands. It is coded according to the following table.

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning |
|---|---|---|---|---|---|---|---|---|
| 0 | - | - | - | - | - | - | - | Last (or only) command |
| 1 | - | - | - | - | - | - | - | More INSTALL commands |
| - | 1 | 0 | 0 | 0 | 0 | 0 | 0 | For registry update |
| - | 0 | 1 | 0 | 0 | 0 | 0 | 0 | For personalization |
| - | 0 | 0 | 1 | 0 | 0 | 0 | 0 | For extradition |
| - | 0 | 0 | 0 | 1 | - | - | 0 | For make selectable |
| - | 0 | 0 | 0 | - | 1 | - | 0 | For install |
| - | 0 | 0 | 0 | - | - | 1 | 0 | For load |

**Table 11-41: INSTALL Command Reference Control Parameter P1**

Bits b8 to b1 shall be coded as follows:

**b8 = 1** indicates that the command data is one of a sequence of components (and not the last), **b8 = 0** indicates that it is the last (or only) component.

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0160

**b7 = 1** indicates that the GlobalPlatform Registry is to be updated, or that functions are to be restricted.

**b6 = 1** indicates that the currently selected Security Domain shall personalize one of its associated Applications and a subsequent STORE DATA command is to be expected

**b5 = 1** indicates that the Application shall be extradited.

**b4 = 1** indicates that the Application shall be made selectable. This applies to an Application being installed or an Application that is already installed.

**b3 = 1** indicates that the Application shall be installed.

**b2 = 1** indicates that the Load File shall be loaded. A subsequent LOAD command is to be expected.

A combination of the [for install] and [for make selectable] options may apply. A combination of the [for load], [for install] and [for make selectable] options may also apply.

#### 11.5.2.2 Reference Control Parameter P2

The reference control parameter P2 shall be set as follows:

**'00'** indicates that no information is provided.

**'01'** indicates the beginning of the combined Load, Install and Make Selectable process.

**'03'** indicates the end of the combined Load, Install and Make Selectable process.

#### 11.5.2.3 Data Field Sent in the Command Message

The data field of the command message contains LV coded data. The LV coded data is represented without delimiters.

##### 11.5.2.3.1 Data Field for INSTALL [for load]

The following table details the INSTALL [for load] command data field. It also applies to the first combined INSTALL [for load, install and make selectable] command data field.

| Name | Length | Value | Presence |
|---|---|---|---|
| Length of Load File AID | 1 | '05' - '10' | Mandatory |
| Load File AID | 5-16 | 'xxxx...' | Mandatory |
| Length of Security Domain AID | 1 | '00' or '05' - '10' | Mandatory |
| Security Domain AID | 0 or 5-16 | 'xxxx...' | Conditional |
| Length of Load File Data Block Hash | 1 | '00' - '7F' | Mandatory |
| Load File Data Block Hash | 0-n | 'xxxx...' - see appendix C.2 | Conditional |
| Length of Load Parameters field | 1-2 | '00' - '7F', or '81 80' - '81 FF' | Mandatory |
| Load Parameters field | 0-n | 'xxxx...' - see section 11.5.2.3.7 | Conditional |
| Length of Load Token | 1-3 | '00' - '80', or '81 80' - '81 FF', or '82 01 00' - '82 FF FF' | Mandatory |

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0161

| Name | Length | Value | Presence |
|---|---|---|---|
| Load Token | 0-n | 'xxxx...' - see appendix C.4.1 | Conditional |

**Table 11-42: INSTALL [for load] Command Data Field**

The Load Token is mandatory for Delegated Management (except for the combined [for load, install and make selectable] command), and for Authorized Management if the off-card entity is not the Security Domain Provider. In all other cases an error status shall be returned if a Load Token is present. The length field for a Load Token is as defined for ASN.1 BER-TLV (see ISO 8825-1) except that the length 128 may also be coded on one byte as '80'.

The Load File Data Block Hash is mandatory if a Load Token is present or if the Load File contains one or more DAP Blocks. In all other cases, the Load File Data Block Hash is optional and may be verified by the card.

The Load File AID and the Load Parameters shall be consistent with the information contained in the Load File Data Block (if any).

#### 11.5.2.3.2 Data Field for INSTALL [for install]

The following table details the INSTALL [for install] command data field. It also applies to the final combined [for load, install and make selectable] command data field.

| Name | Length | Value | Presence |
|---|---|---|---|
| Length of Executable Load File AID | 1 | '00' or '05' - '10' | Mandatory |
| Executable Load File AID | 0 or 5-16 | 'xxxx...' | Conditional |
| Length of Executable Module AID | 1 | '00' or '05' - '10' | Mandatory |
| Executable Module AID | 0 or 5-16 | 'xxxx...' | Conditional |
| Length of Application AID | 1 | '05' - '10' | Mandatory |
| Application AID | 5-16 | 'xxxx...' | Mandatory |
| Length of Privileges | 1 | '01', '03' | Mandatory |
| Privileges | 1, 3 | byte 1 - byte 2 – byte 3: see section 11.1.2 | Mandatory |
| Length of Install Parameters field | 1-2 | '02' - '7F' or '81 80' - '81 FF' | Mandatory |
| Install Parameters field | 2-n | 'xxxx' - see section 11.5.2.3.7 | Mandatory |
| Length of Install Token | 1-3 | '00' - '80', or '81 80' - '81 FF', or '82 01 00' - '82 FF FF' | Mandatory |
| Install Token | 0-n | 'xxxx...' - see appendix C.4.2 or C.4.7 | Conditional |

**Table 11-43: INSTALL [for install] Command Data Field**

The Install Token is mandatory for Delegated Management and for Authorized Management if the off-card entity is not the Security Domain Provider. In all other cases an error status shall be returned if an Install Token is present. The length field for the Install Token is formatted as defined by ASN.1 BER-TLV (see ISO 8825-1) except that the length 128 may also be coded on one byte as '80'.

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0162

The presence of the Executable Load File AID is optional for the combined Load, Install and Make Selectable command. If present it shall match the Load File AID of the first combined Load, Install and Make Selectable command.

The Executable Module AID is the AID of the Executable Module previously loaded. The presence of the Executable Module depends on the requirements of the Run Time Environment.

GlobalPlatform cards use the instance AID to indicate the AID with which the installed Application will be selected.

The presence of the Privileges is required. If an Application is only being installed and not made selectable with the same INSTALL command the Card Reset privilege cannot be set.

The instance AID, the Privileges and the Application Specific Parameters shall be made known to the Application.

Note for backward compatibility: when receiving Privileges coded on one byte for any Application or Security Domain, the OPEN shall assign the second byte with the default values defined in section 6.6.2.

#### 11.5.2.3.3 Data Field for INSTALL [for make selectable]

The following table details the INSTALL [for make selectable] command data field.

| Name | Length | Value | Presence |
|---|---|---|---|
| Length of data | 1 | '00' | Mandatory |
| Length of data | 1 | '00' | Mandatory |
| Length of Application AID | 1 | '05' - '10' | Mandatory |
| Application AID | 5-16 | 'xxxx...' | Mandatory |
| Length of Privileges | 1 | '01', '03' | Mandatory |
| Privileges | 1, 3 | byte 1 - byte 2 – byte 3: see section 11.1.2 | Mandatory |
| Length of Make Selectable Parameters field | 1 | '00' - '7F' | Mandatory |
| Make Selectable Parameters field | 0-n | 'xxxx' - see section 11.5.2.3.7 | Conditional |
| Length of Make Selectable Token | 1-3 | '00' - '80', or '81 80' - '81 FF', or '82 01 00' - '82 FF FF' | Mandatory |
| Make Selectable Token | 0-n | 'xxxx...' - see appendix C.4.3 | Conditional |

**Table 11-44: INSTALL [for make selectable] Command Data Field**

If the Card Reset privilege is set in the Privileges field, the GlobalPlatform Registry shall be updated according to the rules defined in section 6.6 - *Privileges*. Any other privilege set in the Privileges field, regardless of its length, shall be ignored by the card.

The Make Selectable Token is mandatory for Delegated Management, and for Authorized Management if the off-card entity is not the Security Domain Provider. In all other cases an error status shall be returned if a Make Selectable Token is present. The length field for the Make Selectable Token is as defined for ASN.1 BER-TLV (see ISO 8825-1) except that the length 128 may also be coded on one byte as '80'.

#### 11.5.2.3.4 Data Field for INSTALL [for extradition]

The following table details the INSTALL [for extradition] command data field.

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0163

| Name | Length | Value | Presence |
|---|---|---|---|
| Length of Security Domain AID | 1 | '05' - '10' | Mandatory |
| Security Domain AID | 5-16 | 'xxxx...' | Mandatory |
| Length of data | 1 | '00' | Mandatory |
| Length of Application or Executable Load File AID | 1 | '05' - '10' | Mandatory |
| Application or Executable Load File AID | 5-16 | 'xxxx...' | Mandatory |
| Length | 1 | '00' | Mandatory |
| Length of Extradition Parameters field | 1 | '00' - '7F' | Mandatory |
| Extradition Parameters field | 0-n | 'xxxx' - see section 11.5.2.3.7 | Conditional |
| Length of Extradition Token | 1-3 | '00' - '80', or '81 80' - '81 FF', or '82 01 00' - '82 FF FF' | Mandatory |
| Extradition Token | 0-n | 'xxxx...' - see appendix C.4.4 | Conditional |

**Table 11-45: INSTALL [for extradition] Command Data Field**

The Security Domain AID indicates to which Security Domain this Application or Executable Load File is being extradited. The Security Domain with which this Application or Executable Load File is currently associated is the currently selected Application.

The Extradition Token is mandatory for Delegated Management, and for Authorized Management if the off-card entity is not the Security Domain Provider. In all other cases an error status shall be returned if an Extradition Token is present. The length field for the Extradition Token is as defined for ASN.1 BER-TLV (see ISO 8825-1) except that the length 128 may also be coded on one byte as '80'.

#### 11.5.2.3.5 Data Field for INSTALL [for registry update]

The following table details the INSTALL [for registry update] command data field.

| Name | Length | Value | Presence |
|---|---|---|---|
| Length of Security Domain AID | 1 | '00' or '05' - '10' | Mandatory |
| Security Domain AID | 0 or 5-16 | 'xxxx...' | Conditional |
| Length of data | 1 | '00' | Mandatory |
| Length of Application AID | 1 | '00' or '05' - '10' | Mandatory |
| Application AID | 0 or 5-16 | 'xxxx...' | Conditional |
| Length of Privileges | 1 | '00', '01; '03' | Mandatory |
| Privileges | 0, 1, 3 | byte 1 - byte 2 – byte 3: see section 11.1.2 | Conditional |
| Length of Registry Update Parameters field | 1 | '00' - '7F' | Mandatory |
| Registry Update Parameters field | 0-n | 'xxxx' - see section 11.5.2.3.7 | Conditional |
| Length of Registry Update Token | 1-3 | '00' - '80', or '81 80' - '81 FF', or '82 | Mandatory |

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0164

| Name | Length | Value | Presence |
|---|---|---|---|
| | | 01 00' - '82 FF FF' | |
| Registry Update Token | 0-n | 'xxxx...' - see appendix 0 | Conditional |

**Table 11-46: INSTALL [for registry update] Command Data Field**

The Security Domain AID, if present, indicates to which Security Domain this Application is being extradited. The Security Domain with which this Application is currently associated is the currently selected Application. The Application AID shall be present except when modifying the functionality of the OPEN.

For updating or revoking privileges the Privileges field shall be present. For updating implicit selection parameters or service parameters the corresponding tag within the Registry Update Parameters field shall be present - see section 11.5.2.3.7.

The Registry Update Token is mandatory for Delegated Management, and for Authorized Management if the off-card entity is not the Security Domain Provider. In all other cases an error status shall be returned if a Registry Update Token is present. The length field for the Registry Update Token is as defined for ASN.1 BER-TLV (see ISO 8825-1) except that the length 128 may also be coded on one byte as '80'.

All modifications requested in the INSTALL [for registry update] command data field (e.g. registry updates and extradition) shall either all succeed or no update shall occur if any one of the updates would fail for any reason.

#### 11.5.2.3.6 Data Field for INSTALL [for personalization]

The following table details the INSTALL [for personalization] command data field.

| Name | Length | Value | Presence |
|---|---|---|---|
| Length of data | 1 | '00' | Mandatory |
| Length of data | 1 | '00' | Mandatory |
| Length of Application AID | 1 | '05' - '10' | Mandatory |
| Application AID | 5-16 | 'xxxx...' | Mandatory |
| Length of data | 1 | '00' | Mandatory |
| Length of data | 1 | '00' | Mandatory |
| Length of data | 1 | '00' | Mandatory |

**Table 11-47: INSTALL [for personalization] Command Data Field**

#### 11.5.2.3.7 INSTALL Command Parameters

The Load and Install Parameters fields are TLV structured values including optional System Specific Parameters and Application Specific Parameters. While the presence of the System Specific Parameters is optional for both loading and installation, even if they are present, it is not required that the system take heed of these i.e. their presence shall be anticipated but the content may be ignored.

In all cases, the presence of the data objects in tag 'B6' and the sub-tags '42', '45', 5F20' and '93' is strongly recommended when using asymmetric Secure Channel Protocol '10'.

The following table identifies the possible tags for use in the Load Parameters field of the INSTALL [for load] command:

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0165

| Tag | Length | Name | Presence |
|---|---|---|---|
| 'EF' | 1-n | System Specific Parameters | Conditional |
| 'C6' | 2 or 4 | Non volatile code Minimum Memory requirement | Optional |
| 'C7' | 2 or 4 | Volatile data Minimum Memory requirement | Optional |
| 'C8' | 2 or 4 | Non volatile data Minimum Memory requirement | Optional |
| 'CD' | 1 | Load File Data Block format id | Optional |
| 'DD' | 1-n | Load File Data Block Parameters | Conditional |
| 'B6' | 1-n | Control Reference Template for Digital Signature (Token) | Conditional |
| '42' | 1-n | Identification Number of the Security Domain with the Token Verification privilege | Optional |
| '45' | 1-n | Image Number of the Security Domain with the Token Verification privilege | Optional |
| '5F20' | 1-n | Application Provider identifier | Optional |
| '93' | 1-n | Token identifier/number (digital signature counter) | Optional |

**Table 11-48: Load Parameter Tags**

Some of the data objects in Load Parameters relate to memory management, which is an optional feature of a card. A Memory Management data object is a data object that represents an amount of memory resources counted in bytes. The minimum memory requirements (tags 'C6', 'C7' and 'C8') are coded as a 2-byte integer for values up to 32767 and a 4-byte integer above 32767 - see section 9.7 - *Memory Resource Management*. When present, the Provider id (tag '5F20') shall be registered in the GlobalPlatform Registry.

The presence of Load File Data Block Parameters depends on the value of Load File Data Block format id.

The following table identifies the possible tags for use in the Install Parameters field of the INSTALL [for install] command:

| Tag | Length | Name | Presence |
|---|---|---|---|
| 'C9' | 1-n | Application Specific Parameters | Mandatory |
| 'EF' | 1-n | System Specific Parameters | Conditional |
| 'C7' | 2 or 4 | Volatile Memory Quota | Optional |
| 'C8' | 2 or 4 | Non volatile Memory Quota | Optional |
| 'CB' | 2-n | Global Service Parameters | Optional |

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0166

| Tag | Length | Name | Presence |
|---|---|---|---|
| 'D7' | 2 | Volatile Reserved Memory | Optional |
| 'D8' | 2 | Non volatile Reserved Memory | Optional |
| 'CA' | 1-n | TS 102 226 specific parameter | Optional |
| 'CF' | 1 | Implicit selection parameter | See note below |
| 'EA' | 1-n | TS 102 226 specific template | Optional |
| 'B6' | 1-n | Control Reference Template for Digital Signature (Token) | Conditional |
| '42' | 1-n | Identification Number of the Security Domain with the Token Verification privilege | Optional |
| '45' | 1-n | Image Number of the Security Domain with the Token Verification privilege | Optional |
| '5F20' | 1-n | Application Provider identifier | Optional |
| '93' | 1-n | Token identifier/number (digital signature counter) | Optional |

**Table 11-49: Install Parameter Tags**

Note: Tag 'CF' may be present in Install Parameters for the combined INSTALL [for install and make selectable] command and in the final combined INSTALL [for load, install and make selectable] command. Tag 'CF' may be occur in multiple INSTALL commands, appending to the collection of implicit selection parameters for the Application. Implicit Selection parameters cannot be deleted.

Some of the data objects in Install Parameters relate to memory management, which is an optional feature of a card. A Memory Management data object is a data object that represents an amount of memory resources counted in bytes. The memory quota values (tags 'C7' and 'C8') are coded as a 2-byte integer for values up to 32767 and a 4-byte integer above 32767 - see section 9.7 - *Memory Resource Management*.

When present, the Provider id (tag '5F20') shall be registered in the GlobalPlatform Registry.

When present in the INSTALL [for install] command, the information contained in tag 'C9' (length + data) shall be passed to the Application being installed.

When present in the INSTALL [for install] command, the information contained in tag 'CB' shall comprise one or more two-byte service parameters as defined in section 8.1.3 - *Global Service Parameters*.

The following table identifies the possible tags for use in the Make Selectable Parameters field of the INSTALL [for make selectable] command:

| Tag | Length | Name | Presence |
|---|---|---|---|
| 'EF' | 1-n | System Specific Parameters | Conditional |
| 'CF' | 1 | Implicit selection parameter | Optional |
| 'B6' | 1-n | Control Reference Template for Digital Signature (Token) | Conditional |
| '42' | 1-n | Identification Number of the Security Domain with the Token Verification | Optional |

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0167

| Tag | Length | Name | Presence |
|---|---|---|---|
| | | privilege | |
| '45' | 1-n | Image Number of the Security Domain with the Token Verification privilege | Optional |
| '5F20' | 1-n | Application Provider identifier | Optional |
| '93' | 1-n | Token identifier/number (digital signature counter) | Optional |

**Table 11-50: Make Selectable Parameter Tags**

The following table identifies the possible tags for use in the Extradition Parameters field of the INSTALL [for extradition] command:

| Tag | Length | Name | Presence |
|---|---|---|---|
| 'B6' | 1-n | Control Reference Template for Digital Signature (Token) | Conditional |
| '42' | 1-n | Identification Number of the Security Domain with the Token Verification privilege | Optional |
| '45' | 1-n | Image Number of the Security Domain with the Token Verification privilege | Optional |
| '5F20' | 1-n | Application Provider identifier | Optional |
| '93' | 1-n | Token identifier/number (digital signature counter) | Optional |

**Table 11-51: Extradition Parameter Tags**

The following table identifies the possible tags for use in the Registry Update Parameters field of the INSTALL [for registry update] command:

| Tag | Length | Name | Presence |
|---|---|---|---|
| 'EF' | 1-n | System Specific Parameters | Conditional |
| 'CF' | 1 | Implicit selection parameter | Optional |
| 'CB' | 2-n | Global Service Parameters | Optional |
| 'D9' | 1 | Restrict Parameter (see Table 11-53) | Conditional |
| 'B6' | 1-n | Control Reference Template for Digital Signature (Token) | Conditional |
| '42' | 1-n | Identification Number of the Security Domain with the Token Verification privilege | Optional |
| '45' | 1-n | Image Number of the Security Domain with the Token Verification privilege | Optional |
| '5F20' | 1-n | Application Provider identifier | Optional |
| '93' | 1-n | Token identifier/number (digital signature counter) | Optional |

**Table 11-52: Registry Update Parameter Tags**

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0168

When no Application AID is present in the INSTALL [for registry update] command, the Restrict Parameter (tag ‘D9’) applies to OPEN. The effects of this function shall be irreversible. When an Application AID is present in the INSTALL [for registry update] command, the Restrict Parameter (tag ‘D9’) applies to the specific Security Domain identified by the Application AID.

If the Restrict Parameter is present and the card does not implement the option the card shall reject the command.

The Restrict Parameter (tag 'D9') lists the functionalities that shall be disabled. Table 11-53 indicates the functionalities that could possibly be disabled.

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning |
|---|---|---|---|---|---|---|---|---|
| X | - | - | - | - | - | - | - | RFU |
| - | 1 | - | - | - | - | - | - | Registry Update |
| - | - | 1 | - | - | - | - | - | Personalization |
| - | - | - | 1 | - | - | - | - | Extradition |
| - | - | - | - | 1 | - | - | - | Make selectable |
| - | - | - | - | - | 1 | - | - | Install |
| - | - | - | - | - | - | 1 | - | Load |
| - | - | - | - | - | - | - | 1 | Delete |

**Table 11-53: Values for Restrict Parameter (Tag 'D9')**

## 11.5.3 Response Message

A data field shall always be returned in the response message. Confirmation data or a single byte of '00' may be returned.

### 11.5.3.1 Data Field Returned in the Response Message

If an INSTALL [for load] command, an INSTALL [for make selectable] command alone or an INSTALL [for personalization] command is being issued, a single byte of '00' shall be returned indicating that no additional data is present.

For INSTALL [for install], INSTALL [for install and make selectable] and INSTALL [for registry update] commands being issued to a Security Domain with the Delegated Management privilege, the data field may contain the confirmation of the install procedure. The overall length of the response message shall not exceed 256 bytes.

The following table describes the structure of the INSTALL response data field. The length field for the Install Confirmation is coded according to ASN.1 BER-TLV (see ISO 8825-1).

| Name | Length | Value | Presence |
|---|---|---|---|
| Length of Install Confirmation | 1-2 | '00' - '7F' or '81 80' - '81 FF' | Mandatory |
| Install Confirmation | 0-n | 'xxxx...' - see section 11.1.6 | Conditional |

**Table 11-54: INSTALL Response Data Field**

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0169

#### 11.5.3.2 Processing State Returned in the Response Message

A successful execution of the command shall be indicated by status bytes '90' '00'.

This command may either return a general error condition as listed in section 11.1.3 - *General Error Conditions* or one of the following error conditions.

| SW1 | SW2 | Meaning |
|---|---|---|
| '65' | '81' | Memory failure |
| '6A' | '80' | Incorrect parameters in data field |
| '6A' | '84' | Not enough memory space |
| '6A' | '88' | Referenced data not found |

**Table 11-55: INSTALL Error Conditions**

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0170

# 11.6 LOAD Command

## 11.6.1 Definition and Scope

This section defines the structure of the Load File transmitted in the LOAD command data field for loading a Load File. The runtime environment internal handling or storage of the Load File is beyond the scope of this Specification.

Multiple LOAD commands may be used to transfer a Load File to the card. The Load File is divided into smaller components for transmission. Each LOAD command shall be numbered starting at '00'. The LOAD command numbering shall be strictly sequential and increments by one. The card shall be informed of the last block of the Load File.

After receiving the last block of the Load File, the card shall execute the internal processes necessary for the Load File and any additional processes identified in the INSTALL [for load] command that preceded the LOAD commands.

## 11.6.2 Command Message

The LOAD command message is coded according to the following table.

| Code | Value | Meaning |
|---|---|---|
| CLA | '80' - '8F', 'C0' - 'CF' or 'E0' - 'EF' | See section 11.1.4 |
| INS | 'E8' | LOAD |
| P1 | 'xx' | Reference control parameter P1 |
| P2 | 'xx' | Block number |
| Lc | 'xx' | Length of data field |
| Data | 'xxxx..' | Load data (and MAC if present) |
| Le | '00' | |

**Table 11-56: LOAD Command Message Structure**

### 11.6.2.1 Reference Control Parameter P1

The following table describes the coding of the reference control parameter P1 indicating whether the block contained in the command message is one in a sequence of blocks or the last block in the sequence.

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning |
|---|---|---|---|---|---|---|---|---|
| 0 | - | - | - | - | - | - | - | More blocks |
| 1 | - | - | - | - | - | - | - | Last block |
| - | X | X | X | X | X | X | X | RFU |

**Table 11-57: LOAD Command Reference Control Parameter P1**

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0171

#### 11.6.2.2 Reference Control Parameter P2 – Block Number

Reference control parameter P2 contains the block number, and shall be coded sequentially from '00' to 'FF'.

#### 11.6.2.3 Data Field Sent in the Command Message

The data field of the command message contains a portion of the Load File.

A complete GlobalPlatform Load File is structured as defined in the following table:

| Tag | Length | Name | Presence |
|---|---|---|---|
| 'E2' | 1-n | DAP Block | Conditional |
| '4F' | 5-16 | Security Domain AID | Mandatory |
| 'C3' | 1-n | Load File Data Block Signature | Mandatory |
| : | : | : | |
| : | : | : | |
| 'E2' | 1-n | DAP Block | Conditional |
| '4F' | 5-16 | Security Domain AID | Mandatory |
| 'C3' | 1-n | Load File Data Block Signature | Mandatory |
| 'C4' | 1-n | Load File Data Block | Conditional |
| 'D4' | 1-n | Ciphered Load File Data Block | Conditional |

**Table 11-58: Load File Structure**

The data objects defined in Table 11-58 shall be coded according to ASN.1 Basic Encoding Rules, and in particular, the length fields (e.g. one byte for length values up to 127).

A DAP Block shall be present within a Load File if the associated Security Domain has the DAP Verification privilege or a Security Domain with the Mandated DAP Verification privilege is present. A properly constructed DAP Block shall contain the Security Domain AID and the Load File Data Block Signature.

A Load File may contain multiple DAP Blocks; each DAP Block being introduced by tag 'E2' and preceding the Load File Data Block.

If the associated Security Domain has the Ciphered Load File Data Block privilege, the Load File Data Block shall be sent encrypted using tag 'D4', otherwise the Load File Data Block shall be sent unencrypted using tag 'C4'. The encryption algorithm of the Ciphered Load File Data Block is configuration dependent.

### 11.6.3 Response Message

A data field shall always be returned in the response message. The content of the data field is only relevant in the case of Delegated Management i.e. if a last LOAD command is being issued to a Security Domain with the Delegated Management privilege, a Receipt may be present in the data field depending on the security policy of the Card Issuer.

#### 11.6.3.1 Data Field Returned in the Response Message

If the LOAD command does not contain the last block in the sequence, a single byte of '00' shall be returned indicating that no additional data is present.

If the Issuer Security Domain processes the LOAD command containing the last block in the sequence, a single byte of '00' shall be returned indicating that no additional data is present.

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0172

For a LOAD command containing the last block in the sequence being issued to a Security Domain with the Delegated Management privilege, the data field may contain the confirmation of the load procedure. The overall length of the response message shall not exceed 256 bytes.

The following table describes the structure of the LOAD response data field. The length field for the Load Confirmation is coded according to ASN.1 BER-TLV (see ISO 8825-1).

| Name | Length | Value | Presence |
|---|---|---|---|
| Length of Load Confirmation | 1-2 | '00' - '7F' or '81 80' - '81 FF' | Mandatory |
| Load Confirmation | 0-n | 'xxxx...' - see section 11.1.6 | Conditional |

**Table 11-59: LOAD Response Data Field**

#### 11.6.3.2 Processing State Returned in the Response Message

A successful execution of the command shall be indicated by status bytes '90' '00'.

This command may either return a general error condition as listed in section 11.1.3 - *General Error Conditions* or one of the following error conditions.

| SW1 | SW2 | Meaning |
|---|---|---|
| '65' | '81' | Memory failure |
| '6A' | '84' | Not enough memory space |

**Table 11-60: LOAD Error Conditions**

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0173

# 11.7 MANAGE CHANNEL Command

## 11.7.1 Definition and Scope

The MANAGE CHANNEL command is processed by the OPEN on cards that are aware of logical channels. It is used to open and close Supplementary Logical Channels. The Basic Logical Channel (channel number zero) can never be closed.

## 11.7.2 Command Message

The MANAGE CHANNEL command message shall be coded according to the following table.

| Code | Value | Meaning |
|---|---|---|
| CLA | '00' - '03' or '40' - '4F' | See section 11.1.4 |
| INS | '70' | MANAGE CHANNEL |
| P1 | 'xx' | Reference control parameter P1 |
| P2 | 'xx' | Reference control parameter P2 |
| Lc | | Not present |
| Le | | '01' if P1 = '00' and not present if P1 = '80' |

**Table 11-61: MANAGE CHANNEL Command Message**

### 11.7.2.1 Reference Control Parameter P1

Reference control parameter P1 is used to indicate whether a Supplementary Logical Channel is being opened or closed.

The following values of the reference control parameter may apply:

**'80'** – Close the Supplementary Logical Channel identified in reference control parameter P2.

**'00'** – Open the next available Supplementary Logical Channel.

### 11.7.2.2 Reference Control Parameter P2

If a Supplementary Logical Channel is being closed (reference control parameter P1 is '80'), the reference control parameter P2 identifies the Supplementary Logical Channel to be closed (i.e. '01', '02' or '03'). For a card supporting further interindustry logical channels, the reference control parameter may identify further interindustry Supplementary Logical Channels (i.e. ‘04’ to ‘13’).

If a Supplementary Logical Channel is being opened (reference control parameter P1 is '00'), the reference control parameter P2 indicates that the next available Supplementary Logical Channel is being opened (i.e. '00').

A card supporting logical channel assignment by off-card entities may accept a reference control parameter P2 indicating the Supplementary Logical Channel number to be opened (i.e. '01', '02' or '03'). A card supporting further interindustry logical channel assignment by off-card entities may accept a reference control parameter P2 indicating the further interindustry Supplementary Logical Channel number to be opened (i.e. ‘04’ to ‘13’).

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0174

#### 11.7.2.3 Data Field Sent in the Command Message

The data field of the command message is not present.

### 11.7.3 Response Message

#### 11.7.3.1 Data Field Returned in the Response Message

The data field of the response message is only present if a Supplementary Logical Channel is being opened.

Depending on the number of logical channels supported by the card, the following values of the data field of the response message may apply:

**'01', '02' or '03'** – Supplementary Logical Channel opened.

For a card supporting further interindustry logical channels, and depending on the number of Supplementary Logical Channels supported by the card, the following values of the data field of the response message may apply:

**'04' to '13'** – Supplementary Logical Channel opened.

#### 11.7.3.2 Processing State Returned in the Response Message

A successful execution of the command shall be indicated by status bytes '90' '00'.

The command may return the following warning:

| SW1 | SW2 | Meaning |
|---|---|---|
| '62' | '00' | Logical Channel already closed |

**Table 11-62: MANAGE CHANNEL Warning Conditions**

This command may either return a general error condition as listed in section 11.1.3 - *General Error Conditions* or one of the following error conditions.

| SW1 | SW2 | Meaning |
|---|---|---|
| '68' | '82' | Secure messaging not supported |
| '6A' | '81' | Function not supported e.g. card Life Cycle State is CARD_LOCKED |

**Table 11-63: MANAGE CHANNEL Error Conditions**

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0175

# 11.8 PUT KEY Command

## 11.8.1 Definition and Scope

The PUT KEY command is used to either:

- Replace an existing key with a new key: The new key has the same or a different Key Version Number but the same Key Identifier as the key being replaced;
- Replace multiple existing keys with new keys: The new keys have the same or a different Key Version Number (identical for all new keys) but the same Key Identifiers as the keys being replaced;
- Add a single new key: The new key has a different combination Key Identifier / Key Version Number than that of the existing keys;
- Add multiple new keys: The new keys have different combinations of Key Identifiers / Key Version Number (identical to all new keys) than that of the existing keys;

When the key management operation requires multiple PUT KEY commands, chaining of the multiple PUT KEY commands is recommended to ensure integrity of the operation.

In this version of the Specification the public values of asymmetric keys are presented in clear text.

## 11.8.2 Command Message

The PUT KEY command message is coded according to the following table:

| Code | Value | Meaning |
|---|---|---|
| CLA | '80' - '8F',<br>'C0' - 'CF' or<br>'E0' - 'EF' | See section 11.1.4 |
| INS | 'D8' | PUT KEY |
| P1 | 'xx' | Reference control parameter P1 |
| P2 | 'xx' | Reference control parameter P2 |
| Lc | 'xx' | Length of data field |
| Data | 'xxxx..' | Key data (and MAC if present) |
| Le | '00' | |

**Table 11-64: PUT KEY Command Message**

### 11.8.2.1 Reference Control Parameter P1

Reference control parameter P1 defines a Key Version Number and whether more PUT KEY commands will follow this one.

The Key Version Number identifies a key or group of keys that is already present on the card. A value of '00' indicates that a new key or group of keys is being added. (The new Key Version Number is indicated in the data field of the command message).

The Key Version Number is coded from '01' to '7F'.

The reference control parameter P1 of the PUT KEY command message is coded according to the following table:

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0176

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning |
|---|---|---|---|---|---|---|---|---|
| 0 | - | - | - | - | - | - | - | Last (or only) command |
| 1 | - | - | - | - | - | - | - | More PUT KEY commands |
| - | X | X | X | X | X | X | X | Key Version Number |

**Table 11-65: PUT KEY Reference Control Parameter P1**

#### 11.8.2.2 Reference Control Parameter P2

Reference control parameter P2 defines a Key Identifier and whether one or multiple keys are contained in the data field.

When one key is contained in the command message data field, reference control parameter P2 indicates the Key Identifier of this key. When multiple keys are contained in the command message data field, reference control parameter P2 indicates the Key Identifier of the first key in the command data field. Each subsequent key in the command message data field has an implicit Key Identifier that is sequentially incremented by one, starting from this first Key Identifier.

The Key Identifier is coded from '00' to '7F'.

The reference control parameter P2 of the PUT KEY command message is coded according to the following table:

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning |
|---|---|---|---|---|---|---|---|---|
| 0 | - | - | - | - | - | - | - | Single key |
| 1 | - | - | - | - | - | - | - | Multiple keys |
| - | X | X | X | X | X | X | X | Key Identifier |

**Table 11-66: PUT KEY Reference Control Parameter P2**

#### 11.8.2.3 Data Field Sent in the Command Message

The command message data field contains a new Key Version Number (coded from '01' to '7F') followed by one or multiple key data fields as represented in the following diagram (with optionally a second and third keys):

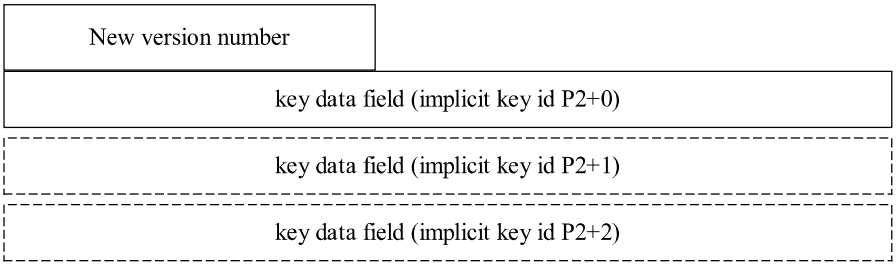



**Table 11-67: Key Version Number Diagram**

The new Key Version Number defines either:

- The version number of a new key or group of keys to be created on the card (Key Version Number indicated in P1 is set to zero); or
- The version number of a new key or group of keys that will replace an existing key or group of keys (Key Version Number indicated in P1 is different from zero).

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0177

If the data field contains multiple keys, the keys all share the same Key Version Number and the sequence in the command data field reflects the incremental sequence of the Key Identifiers.

The format of the key data field depends on the value of the first data element, Key Type.

#### 11.8.2.3.1 Format 1

If the Key Type is coded on one byte (value other than 'FF'), the key data field is structured according to the following table:

| Name | Length | Value | Presence |
|---|---|---|---|
| Key type | 1 | '00' - 'FE' - see section 11.1.8 - *Key Type Coding* | Mandatory |
| Length of key or key component data | 1-3 | '01' - '80', or '81 80' - '81 FF', or '82 01 00' - '82 FF FF' | Mandatory |
| Key or key component data value | 1-n | 'xxxx...' | Mandatory |
| Length of key check value | 1 | '00' - '7F' | Mandatory |
| Key check value | 0-n | 'xxxx...' | Conditional |

**Table 11-68: Key Data Field - Basic**

#### 11.8.2.3.2 Format 2

If the Key Type is coded on two bytes (first byte = 'FF'), the key data field is structured according to the following table:

| Name | Length | Value | Presence |
|---|---|---|---|
| Key type of the first or only key component | 2 | 'FF xx' - see section 11.1.8 - *Key Type Coding* | Mandatory |
| Length of first or only key component | 1-3 | '01' - '80', or '81 80' - '81 FF', or '82 01 00' - '82 FF FF' | Mandatory |
| Key or first key component data value | 1-n | 'xxxx...' | Mandatory |
| | ... | | |
| Key type of the last key component, if more than one | 2 | 'FF xx' - see section 11.1.8 - *Key Type Coding* | Conditional |
| Length of last key component | 1-3 | '01' - '80', or '81 80' - '81 FF', or '82 01 00' - '82 FF FF' | Conditional |
| Last Key component data value | 1-n | 'xxxx…' | Conditional |
| Length of key check value | 1 | '00' - '7F' | Mandatory |
| Key check value (if present) | 0-n | 'xxxx...' | Conditional |
| Length of key usage qualifier | 1 | '00' - '7F' | Mandatory |
| Key usage qualifier | 0-n | 'xxxx...' see section 11.1.9 – Key usage qualifier | Conditional |
| Length of key access | 1 | '00' - '7F' | Mandatory |

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0178

| Name | Length | Value | Presence |
|---|---|---|---|
| Key access | 0-n | 'xxxx...' see section 11.1.10 – Key Access Coding | Conditional |

**Table 11-69: Key Data Field - Extended**

The length of each key component is coded as defined for ASN.1 BER-TLV (see ISO 8825-1) except that the length 128 may also be coded on one byte as '80'.

#### 11.8.2.3.3 Processing Rules

When replacing keys, the new keys shall be presented to the card in the same format as they are already present on the card: in other words, it is not possible to change the size and the associated cryptographic algorithm of an existing key slot.

When using this command to load or replace secret or private keys, the key values shall be encrypted and the reference of the encrypting key and algorithm to be used is known implicitly according to the current context. Public key values may be presented in clear text.

When chaining is used to load or replace a key comprised of more than one component, the subsequent commands must refer to the same Key Identifier and the same Key Version Number as the first PUT KEY command used for the first key component. A key component shall not be split across two PUT KEY commands.

If the data field contains multiple keys or key components, the card must handle the multiple keys or key components in an atomic manner. When PUT KEY commands are chained (i.e. bit b8 of P1 set to 1), the card must handle the multiple key components transferred in the chain of PUT KEY commands (until and including the first PUT KEY command with bit b8 of P1 = 0) in an atomic manner.

The PUT KEY command creates or updates the Key Information Data which may later be returned in tag 'C0', structured as shown in Table 11-27 or Table 11-28.

The modulus component of an RSA key should be the first key component.

It is the responsibility of the receiving on-card entity to verify the key check value when present.

### 11.8.3 Response Message

#### 11.8.3.1 Data Field Returned in the Response Message

The data field of the response message contains in clear text the Key Version Number followed by the key check value(s) not preceded by a length, if any, as presented in the command message data field. The personalization server may use the returned Key Version Number and key check value(s) to verify the correct loading of the key(s).

#### 11.8.3.2 Processing State Returned in the Response Message

A successful execution of the command shall be indicated by status bytes '90' '00'.

This command may either return a general error condition as listed in section 11.1.3 - *General Error Conditions* or one of the following error conditions.

| SW1 | SW2 | Meaning |
|---|---|---|
| '65' | '81' | Memory failure |
| '6A' | '84' | Not enough memory space |

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0179

| SW1 | SW2 | Meaning |
|---|---|---|
| '6A' | '88' | Referenced data not found |
| '94' | '84' | Algorithm not supported |
| '94' | '85' | Invalid key check value |

**Table 11-70: PUT KEY Error Conditions**

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0180

# 11.9 SELECT Command

## 11.9.1 Definition and Scope

The SELECT command is used for selecting an Application. The OPEN only processes SELECT commands indicating the SELECT [by name] option. All options other than SELECT [by name] shall be passed to the currently selected Security Domain or Application on the indicated logical channel.

## 11.9.2 Command Message

The SELECT command is coded according to the following table:

| Code | Value | Meaning |
|---|---|---|
| CLA | '00' - '03' or '40' - '4F' | See section 11.1.4 |
| INS | 'A4' | SELECT |
| P1 | 'xx' | Reference control parameter P1 |
| P2 | 'xx' | Reference control parameter P2 |
| Lc | 'xx' | Length of AID |
| Data | 'xxxx..' | AID of Application to be selected |
| Le | '00' | |

**Table 11-71: SELECT Command Message**

### 11.9.2.1 Reference Control Parameter P1

Reference control parameter P1 shall be coded according to the following table.

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | Select by name |

**Table 11-72: SELECT Reference Control Parameter P1**

A Security Domain or Application may support other values as defined in ISO/IEC 7816-4.

### 11.9.2.2 Reference Control Parameter P2

Reference control parameter P2 shall be coded according to the following table.

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | First or only occurrence |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | Next occurrence |

**Table 11-73: SELECT Reference Control Parameter P2**

OPEN or the underlying runtime environment may support other values as defined in ISO/IEC 7816-4.

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0181

#### 11.9.2.3 Data Field Sent in the Command Message

The data field of the command shall contain the AID of the Application to be selected. The Lc and data field of the SELECT command may be omitted if the Issuer Security Domain is being selected. In this case, Le shall be set to '00' and the command is a case 2 command according to ISO/IEC 7816-4.

### 11.9.3 Response Message

#### 11.9.3.1 Data Field Returned in the Response Message

The SELECT response data field consists of information specific to the selected Application.

The coding of the File Control Information for the Issuer Security Domain and Security Domains shall be according to the following table.

| Tag | Description | Presence |
|---|---|---|
| '6F' | File Control Information (FCI template) | Mandatory |
| '84' | Application / file AID | Mandatory |
| 'A5' | Proprietary data | Mandatory |
| '73' | Security Domain Management Data (see appendix H.3 for detailed coding) | Optional |
| '9F6E' | Application production Life Cycle data | Optional |
| '9F65' | Maximum length of data field in command message | Mandatory |

**Table 11-74: File Control Information**

Additional data objects may be returned within the FCI template.

#### 11.9.3.2 Processing State Returned in the Response Message

A successful execution of the command shall be indicated by status bytes '90' '00'.

The command may return the following warning condition when the Security Domain with the Final Application privilege is being selected.

| SW1 | SW2 | Meaning |
|---|---|---|
| '62' | '83' | Card Life Cycle State is CARD_LOCKED |

**Table 11-75: SELECT Warning Condition**

This command may either return a general error condition as listed in section 11.1.3 - *General Error Conditions* or one of the following error conditions.

| SW1 | SW2 | Meaning |
|---|---|---|
| '68' | '82' | Secure messaging not supported |
| '6A' | '81' | Function not supported e.g. card Life Cycle State is CARD_LOCKED |
| '6A' | '82' | Selected Application / file not found |

**Table 11-76: SELECT Error Conditions**

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0182

# 11.10 SET STATUS Command

## 11.10.1 Definition and Scope

The SET STATUS command shall be used to modify the card Life Cycle State or the Application Life Cycle State.

## 11.10.2 Command Message

The SET STATUS command message is coded according to the following table.

| Code | Value | Meaning |
|---|---|---|
| CLA | '80' - '8F',<br>'C0' - 'CF' or<br>'E0' - 'EF' | See section 11.1.4 |
| INS | 'F0' | SET STATUS |
| P1 | 'xx' | Status type |
| P2 | 'xx' | State control |
| Lc | 'xx' | Length of data field |
| Data | 'xxxxx…' | AID of Application (and MAC if present) |
| Le | | Not present |

**Table 11-77: SET STATUS Command Message**

### 11.10.2.1 Reference Control Parameter P1 - Status Type

The status type of the SET STATUS command message indicates if the change in the Life Cycle State applies to the Issuer Security Domain, Supplementary Security Domains or an Application. The status type can also indicate that the command applies to a Security Domain and all its associated Applications: this only applies for transition to, and back from, the LOCKED state. The status type shall be coded according to the following table.

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning |
|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | - | - | - | - | - | Indicate Issuer Security Domain |
| 0 | 1 | 0 | - | - | - | - | - | Indicate Application or Supplementary Security Domain |
| 0 | 1 | 1 | - | - | - | - | - | Indicate Security Domain and its associated Applications |
| - | - | - | X | X | X | X | X | RFU |

**Table 11-78: SET STATUS – Status Type**

Note: When the SET STATUS command applies for a Security Domain and its Associated Applications, then the SET STATUS command applies to the sub-hierarchy of the Security Domain indicated in the command data field. If the SET STATUS is used to lock all Applications, all Applications remain already locked, and no error status is returned. If the SET STATUS is used to unlock all Applications, all Applications already unlocked remain unlocked, and no error status is returned.

### 11.10.2.2 Reference Control Parameter P2 - State Control

The state control of the SET STATUS command message indicates the state transition required and shall be coded according to section 11.1.1 - *Life Cycle State Coding*.

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0183

For the Issuer Security Domain (which inherits the card Life Cycle State), the parameter shall be coded according to Table 11-6 and abide by the transitioning rules as diagrammed in Figure 5-1. A Security Domain with the Card Terminate or the Card Lock privilege is able to terminate or lock, respectively, the card using the SET STATUS command with P1 set to '80'.

For a Security Domain setting its own Life Cycle State using this command, the only possible transitions are to the PERSONALIZED or LOCKED state: The parameter shall be coded according to Table 11-5.

For an Application setting its own Life Cycle State using this command, the parameter shall be coded according to Table 11-4 and abide by the transitioning rules as depicted in Figure 5-2.

For a Security Domain setting the Life Cycle State of another Application or Supplementary Security Domain, the only possible transitions are to the LOCKED state and subsequently back to the previous state. The only relevant bit of this parameter would therefore be bit b8 (all other bits are ignored):

- b8 = 1 indicates a transition to the LOCKED state;
- b8 = 0 indicates a transition (from LOCKED) back to the previous state.

A request to transition a Security Domain or an Application to its current Life Cycle State shall be rejected.

#### 11.10.2.3 Data Field Sent in the Command Message

The data field shall contain the AID of the target Application or Security Domain for which a Life Cycle change is requested. The on-card entity receiving the command shall be directly or indirectly associated with this target Application or Security Domain or shall have the relevant privilege. If reference control parameter P1 is '80' the content of the command data field shall be ignored. If the command relates to a Security Domain and all its associated Applications, the data field shall contain the AID of the Security Domain.

### 11.10.3 Response Message

#### 11.10.3.1 Data Field Returned in the Response Message

The data field of the response message shall not be present.

#### 11.10.3.2 Processing State Returned in the Response Message

A successful execution of the command shall be indicated by status bytes '90' '00'.

This command may either return a general error condition as listed in section 11.1.3 - *General Error Conditions* or one of the following error conditions.

| SW1 | SW2 | Meaning |
|---|---|---|
| '6A' | '80' | Incorrect values in command data |
| '6A' | '88' | Referenced data not found |

**Table 11-79: SET STATUS Error Conditions**

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0184

# 11.11 STORE DATA Command

## 11.11.1 Definition and Scope

The STORE DATA command is used to transfer data to an Application or the Security Domain processing the command.

The Security Domain determines if the command is intended for itself or an Application depending on a previously received command. If a preceding command was an INSTALL [for personalize] command, the STORE DATA command is destined for an Application.

Multiple STORE DATA commands are used to send data to the Application or Security Domain by breaking the data into smaller components for transmission. The Security Domain shall be informed of the last block.

A personalization session starts when a Security Domain receives a valid INSTALL [for personalize] command designating an Application (implementing either the Application or the Personalization interface) to which the Security Domain shall forward subsequently received STORE DATA commands.

A personalization session ends when:

- The card is reset;
- The Security Domain is deselected (i.e. another, or the same, applet is selected on the same logical channel);
- The Security Domain is selected on the same or another logical channel;
- The Secure Channel session (if any) established by the Security Domain is reset, possibly by the targeted application (see conditions triggering Secure Channel Termination described in section 10.2.3);
- The Security Domain receives an INSTALL [for personalize] command (starting a new personalization session for another application);
- The Security Domain receives a STORE DATA command indicating P1.b8=1 (last block);

Any STORE DATA command received out of such a personalization session shall be processed by the Security Domain itself.

## 11.11.2 Command Message

The STORE DATA command message shall be coded according to the following table.

| Code | Value | Meaning |
|---|---|---|
| CLA | '80' - '8F',<br>'C0' - 'CF' or<br>'E0' - 'EF' | See section 11.1.4 |
| INS | 'E2' | STORE DATA |
| P1 | 'xx' | Reference control parameter P1 |
| P2 | 'xx' | Block number |
| Lc | 'xx' | Length of data field |
| Data | 'xxxxx…' | Application data and MAC (if present) |

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0185

| Code | Value | Meaning |
|---|---|---|
| Le | | Not present |

**Table 11-80: STORE DATA Command Message**

#### 11.11.2.1 Reference Control Parameter P1

Reference control parameter P1 shall be coded according to the following table.

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning |
|---|---|---|---|---|---|---|---|---|
| 0 | - | - | - | - | - | - | - | More blocks |
| 1 | - | - | - | - | - | - | - | Last block |
| - | 0 | 0 | - | - | - | - | - | No general encryption information or non-encrypted data |
| - | 0 | 1 | - | - | - | - | - | Application dependent encryption of the data |
| - | 1 | 0 | - | - | - | - | - | RFU (encryption indicator) |
| - | 1 | 1 | - | - | - | - | - | Encrypted data |
| - | - | - | 0 | 0 | - | - | - | No general data structure information |
| - | - | - | 0 | 1 | - | - | - | DGI format of the command data field |
| - | - | - | 1 | 0 | - | - | - | BER-TLV format of the command data field |
| - | - | - | 1 | 1 | - | - | - | RFU (data structure information) |
| - | - | - | - | - | X | X | X | RFU |

**Table 11-81: STORE DATA Reference Control Parameter P1**

Bits b5 and b4 provide information on the data structure of the command message data field.

- b5 - b4 = 00 indicate that no general information on the data structure is provided, i.e. the data structure is Application dependent;
- b5 - b4 = 01 indicate that the command message data field is coded as one or more DGI structures, according to GlobalPlatform Systems Scripting Language Specification;
- b5 - b4 = 10 indicate that the command message data field is coded as one or more BER-TLV structures, according to ISO 8825.

Bits b7 and b6 provide information on the encryption of the value fields of the data structure present in the command message data field.

- b7 – b6 = 00 indicate that no general information on the data encryption is provided, i.e. the encryption (or non-encryption) of the data is Application dependent, or that the data value fields of all the data structures present in the current command message are not encrypted;
- b7 – b6 = 01 indicate that the encryption (or non-encryption) of the data structure value fields is Application dependent, e.g. when multiple data structures are present in the current command message, some may have encrypted data value fields and other data value fields may be non-encrypted;
- b7 – b6 = 11 indicate that the data value fields of all the data structures present in the current command message are encrypted.

The decryption of application-specific data is the responsibility of the Application.

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0186

#### 11.11.2.2 Reference Control Parameter P2 - Block Number

Reference control parameter P2 shall contain the block number coded sequentially from '00' to 'FF'. The Security Domain shall check the sequence of commands.

#### 11.11.2.3 Data Field Sent in the Command Message

The data field shall contain data in a format expected by the Security Domain or the Application. If the data is intended for an Application, it is sent to the Application as described in section 7.3.3.

Three data structuring modes can be defined:

- Application dependent format applies when no information is available on the format of the incoming command data: bits b5-b4 of reference control parameter P1 are set to '00'. In this case, information on the encryption (or non-encryption) of the incoming command data is usually not available (parameter P1 bits b7-b6 set to '00'): the format and eventual encryption of the incoming command data are implicitly known by the Application;
- DGI formatting applies when all data structures that are present in the command data field are formatted as DGI structures (as defined in the Scripting Specification): bits b5-b4 of reference control parameter P1 are set to '01'. In this case, some information may be available on the encryption (or non-encryption) of the value fields of the DGI data structures: reference control parameter P1 bits b7-b6 are set accordingly;
- BER-TLV formatting applies when all data structures that are present in the command data field are formatted as BER-TLV structures (as defined in ISO 8825): bits b5-b4 of reference control parameter P1 are set to '10'. In this case, some information may be available on the encryption (or non-encryption) of the value fields of the TLV data structures: reference control parameter P1 bits b7-b6 are set accordingly.

If the overall length of the intended command message exceeds 255 bytes, the individual (or group of) data shall be sent in multiple consecutive STORE DATA commands. Whether the data format is a DGI or BER-TLV data structure, the following rules shall apply:

- The data structure length indicators shall always reflect the actual full length of the data structure value field;
- The data structure value field shall be truncated in the STORE DATA command message containing the data structure length indicator (e.g. at the maximum length of the command message);
- The subsequent STORE DATA command shall contain the remainder of the data structure value field (that may be followed by one or more data structure(s) in this same command message) – note: for very large data, more than one subsequent STORE DATA command message may be required for the remainder of the data structure value field;
- The Target Application or Security Domain shall use the last data structure length indicator of a STORE DATA command message to determine whether a subsequent STORE DATA command is expected to contain the remainder of the data structure value field.

The Issuer Security Domain shall support at least the following TLV coded data objects:

- Issuer Identification Number (tag '42')
- Card Image Number (tag '45')
- Issuer Security Domain AID (tag '4F')
- Card Data (tag '66')

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0187

A Supplementary Security Domain should support the following TLV coded data objects:

- Security Domain Provider Identification Number (tag '42')
- Security Domain Image Number (tag '45')
- Security Domain Management Data (tag '66')

When DGI formatting is supported, these data objects may be included in a DGI. In that case, the DGI ‘0070’ shall be used. Otherwise, these data objects shall be presented in their BER-TLV format.

## 11.11.3 Response Message

### 11.11.3.1 Data Field Returned in the Response Message

The data field of the response message shall not be present.

### 11.11.3.2 Processing State Returned in the Response Message

A successful execution of the command shall be indicated by status bytes '90' '00'.

This command may either return a general error condition as listed in section 11.1.3 - *General Error Conditions* or the following error condition.

| SW1 | SW2 | Meaning |
|---|---|---|
| '6A' | '80' | Incorrect values in command data |
| '6A' | '84' | Not enough memory space |
| ‘6A’ | ‘88’ | Referenced data not found |

**Table 11-82: STORE DATA Error Condition**

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0188

# Appendices

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0189

# A GlobalPlatform API

## A.1 GlobalPlatform on a Java Card

This section contains only the API required for GlobalPlatform 2.2.x Java Cards. Use of the Open Platform 2.0.1' API is still allowed for supporting older versions of Applications but is deprecated. It is defined in version 2.1.1 of this Specification.

The deprecated API and new API both access the same objects where applicable. While this may seem obvious for methods that have the same name across both classes (e.g. `setATRHistBytes()`, `setCardContentState()` and `getCardContentState()`) it shall also be noted as for example that an application that uses the `update()` method in the new API to change the value of the global PIN will affect the same global PIN of an application that uses the `setPIN()` method in the deprecated API to verify the global PIN.

#### GlobalPlatform Specific Requirements

In order to ensure the highest level of interoperability of GlobalPlatform implementations, GlobalPlatform also adopts the order defined in section 6.2 - *Java Card™ 2.2.x Virtual Machine Specification*.

Some of the minor modifications to the standard functionality defined in the *Java Card™ 2.1.1 Runtime Environment (JCRE) Specifications* and the *Java Card™ 2.1.1 Application Programming Interface* are no longer relevant with the Java Card™ 2.2.x specifications.

GPRegistryEntry objects shall be implemented as Shareable Interface Objects as defined in section 6.2.4 '*Shareable Interfaces*' of the *Java Card™ 2.2.x Runtime Environment (JCRE) Specification* in order to ensure shared access.

#### GlobalPlatform package AID

Each GlobalPlatform package AID will be a concatenation of a RID and a PIX. The AID value of the Java Card Export File for the new GlobalPlatform API (identical for both GlobalPlatform 2.1 and 2.1.1) based on the RID specified in appendix H - *GlobalPlatform Data Values and Card Recognition Data* is 'A00000015100'.

#### Installation

In section 3.1 - *The Method* `install` of the *Java Card™ 2.2.x Runtime Environment (JCRE) Specifications,* the parameters passed to the method are defined to be initialization parameters from the contents of the incoming byte array parameter.

This specification expands on this requirement and further defines the content of the Install Parameters. This expansion affects both the implementation of an OPEN and the behavior of a Java Card applet developed for a GlobalPlatform card. It does not affect the definition of the `install` method of the Class Applet of the *Java Card™ 2.2.x Application Programming Interface* specification.

The Install Parameters shall identify the following data, present in the INSTALL [for install] command (see section 11.5.2.3.2 - *Data Field for INSTALL [for install]*):

- The instance AID;
- The Privileges;

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0190

- The Application Specific Parameters[1].

The OPEN is responsible for ensuring that the parameters (`bArray, bOffset` and `bLength`) contain the following information:

The array, `bArray`, shall contain the following consecutive LV coded data:

- Length of the instance AID;
- The instance AID;
- Length of the Privileges;
- The Privileges;
- Length of the Application Specific Parameters;
- The Application Specific Parameters.

The byte, `bOffset`, shall contain an offset within the array pointing to the length of the instance AID.

The byte, `bLength`, shall contain a length indicating the total length of the above-defined data in the array.

The applet is required to utilize the instance AID as a parameter when invoking the `register (byte [] bArray, short bOffset, byte bLength)` method of the Class Applet of the *Java Card™ 2.2.x Application Programming Interface* specification.

### T=0 Transmission Protocol

GlobalPlatform cards are intended to be functional in the widest range of environments (i.e. Card Acceptance Devices). Currently the *Java Card™ 2.2.x Runtime Environment (JCRE) Specifications* describe the behavior for case 2 commands (when using the T=0 protocol) in contradiction to EMV 2000. GlobalPlatform mandates that the JCRE shall handle this case of command in accordance with ISO/IEC 7816: An applet receiving a case 2 command builds the response and invokes the appropriate API to output the data. If the data is less than the data expected by the terminal, the OPEN will store the data and output a '6Cxx' response code and wait for the CAD to re-issue the command with the correct length. When the re-issued command is received the JCRE will manage the outputting of the stored data.

### Atomicity

Unless otherwise specified all internal persistent objects of the GlobalPlatform API must conform to a transaction in progress.

All operations performed by this API, except the `Application.processData()` method shall be executed atomically. Objects used to enforce the implementation of velocity checking shall not conform to a transaction in progress.

### Logical channels

The following logical channel restrictions apply to Java Card™ 2.2.x (see the *Java Card™ 2.2.x Runtime Environment (JCRE) Specifications* for more detail):

---

[1] While the APDU command contains Install Parameters representing TLV coded system and Application Specific Parameters, the application only requires knowledge of the Application Specific Parameters i.e. only LV of the TLV coded structure ‘C9’ are present as parameters.

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0191

Selection of an Application on a logical channel as defined in section 6.3 - *Command Dispatch* will be unsuccessful if this same Application, or any other Application instantiated from code in the same package from which the Application being selected was instantiated, is currently selected on another logical channel but the application code does not implement the `MultiSelectable` interface. Security Domains shall implement the `MultiSelectable` interface.

Changing context from a Security Domain to an Application as defined in section 7.3.3 - *Personalization Support* will be unsuccessful if this same Application, or any other Application instantiated from code in the same package from which the Application being personalized was instantiated, is currently selected on another logical channel but the application code does not implement the `MultiSelectable` interface.

An Application that has the Card Reset privilege and is intended for a card that supports Supplementary Logical Channels should implement the `MultiSelectable` interface.

GlobalPlatform only defines the assignment of logical channel numbers by the card. Optionally and as defined in Java Card 2.2, a card may also support assignment of logical channel numbers by the terminal.

### Cryptographic Algorithms

GlobalPlatform cards supporting RSA cryptography should support key sizes not defined as constants in the Key Builder class. More specifically support for key sizes being a multiple of 4 bytes (32 bits), and being within the allowed key lengths defined by the implementation, should be available.

### Level of trust

The Java Card 2.2.x specifications assume that the RID of the AID of packages, applets and instances will be utilized to ensure a level of trust between these entities. In section 4.2.2 - *AID Usage* of the *Java Card™ 2.2.1 Application Programming Interface* it is defined that the RID of an AID of a component must match the RID of the AID of the package and in the definition of the `register (byte [] bArray, short bOffset, byte bLength)` method of the *Java Card™ 2.2.x Application Programming Interface* specification it is defined that an exception must be thrown if the RID portion of the AID bytes in the `bArray` parameter does not match the RID portion of the Java Card name of the applet.

From a real world implementation point of view, mandating that the RID of the instance AID must be the same as the RID of the component from which it was instantiated, is not practical. GlobalPlatform implementations shall not mandate that there be any link through the AID of an instance to its original package. It does however assume that all applications in the same package share the same level of trust.

### Invocation of GlobalPlatform methods

The Application Programming Interface defined herein is accessible to any Java Card applet developed with the intention of being present on a GlobalPlatform card. One limitation does exist relating to the constructor of the applet and to the `install()` method of the Class Applet of the *Java Card™ 2.2.x Application Programming Interface.* As this specification does not define exactly when the instance of an applet becomes an entry in the card's GlobalPlatform Registry, an applet developer can only assume that this has occurred following the successful completion of the install method. To ensure interoperability, GlobalPlatform API methods that require access to the GlobalPlatform Registry entry of the applet invoking the method, shall not be invoked before registering the applet.

The following is a list of methods that may be invoked from within the constructor or the `install()` method:

- getCardState;
- getCVM;
- getService.

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0192

The required behavior of the card in the event that an Application incorrectly invokes a method of the `org.globalplatform.GPSystem` class other than those listed above is undefined. For example, an exception may be thrown and the processing of the `install()` method may be aborted.

**Selection**

On GlobalPlatform cards, if an error occurs during the processing of the `select()` method or if the `select()` method returns `False` or if the Application cannot be selected because it does not implement the `Multiselectable` interface, the OPEN shall continue searching through the GlobalPlatform Registry for a subsequent full or partial match as defined in section 6.4.2.1.2. If no Application is selected, the corresponding logical channel remains open with no currently selected Application. Since no Application is currently selected, any subsequent command, other than a MANAGE CHANNEL or SELECT [by name] command, will be rejected. It is expected that the off-card entity will take appropriate action on such an error, e.g. select another Application, close the corresponding logical channel, reset or power off the card.

The Method Summary and Details for the GlobalPlatform Java Card™ API specification is now available in a separate document which may be found on the GlobalPlatform website.

## A.2 GlobalPlatform on MULTOS™

The GlobalPlatorm on MULTOS™ specification is now available in a separate document which may be found on the GlobalPlatform website.

***Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.***
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0193

# B Algorithms (Cryptographic and Hashing)

A GlobalPlatform card may support many types of security functions for use by applications. This appendix contains examples of several of the cryptographic algorithms and the hashing method that are possible for GlobalPlatform.

## B.1 Data Encryption Standard (DES)

The Data Encryption Standard (DES) is a symmetric cryptographic algorithm that requires the use of the same secret key to encrypt and decrypt data. In its simplest form it uses an 8-byte key to encrypt an 8-byte block of data and the same 8-byte key to decrypt and retrieve the original clear text.

Triple DES uses a compound operation of DES encryption and decryption. Triple DES as used in this specification uses keying option 2 as defined in ISO/IEC 18033-3.

### B.1.1 Encryption/Decryption

For encryption two variants are defined.

#### B.1.1.1 CBC Mode

Triple DES in CBC mode, as defined in [ANSI X9.52] and [ISO 10116], is used with an Initial Chaining Value equal to '00 00 00 00 00 00 00 00'.

#### B.1.1.2 ECB Mode

Triple DES in ECB mode, as defined in [ANSI X9.52] and [ISO 10116], is used.

### B.1.2 MACing

The chaining data encryption methods are defined in [ISO 9797].

#### B.1.2.1 Full Triple DES MAC

The full triple DES MAC is as defined in [ISO 9797-1] as MAC Algorithm 1 with output transformation 3, without truncation, and with triple DES taking the place of the block cipher.

#### B.1.2.2 Single DES Plus Final Triple DES MAC

This is also known as the Retail MAC. It is as defined in [ISO 9797-1] as MAC Algorithm 3 with output transformation 3, without truncation, and with DES taking the place of the block cipher.

## B.2 Hashing Algorithms

A hash is a one-way digest operation over an arbitrary length of data that returns a fixed length hash value. A hash is not a cryptographic algorithm and it only provides integrity of the data. It does not provide authentication or confidentiality.

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0194

### B.2.1 Secure Hash Algorithm (SHA-1)

SHA-1 is defined in [ISO 10118-3] and FIPS PUB 180-1.

### B.2.2 MULTOS Asymmetric Hash Algorithm

The asymmetric hash algorithm for GlobalPlatform on MULTOS is described in MULTOS document [MAO-DOC-REF-009].

## B.3 Public Key Cryptography Scheme 1 (PKCS#1)

Unlike DES, which uses a shared secret key, public key cryptography employs the use of a Private Key (kept secret by one entity) and a Public Key. One public key algorithm used for GlobalPlatform is RSA (Rivest / Shamir / Adleman).

The signature scheme is RSASSA-PKCS-v1_5 as defined in PKCS#1. The hash function is SHA-1.

## B.4 DES Padding

Unless specified to the contrary, padding prior to performing a DES operation across a block of data is achieved in the following manner:

- Append an '80' to the right of the data block;
- If the resultant data block length is a multiple of 8 bytes, no further padding is required;
- Append binary zeroes to the right of the data block until the data block length is a multiple of 8 bytes.

If the data is being padded with the intention of generating a MAC, the padding is discarded following the DES operation.

## B.5 Key Check Values

If required, when loading a secret key to the card, a key check value shall be calculated as described below.

For a DES key, the key check value is computed by encrypting 8 bytes, each with value '00', with the key to be checked and retaining the 3 highest-order bytes of the encrypted result.

For a AES key, the key check value is computed by encrypting 16 bytes, each with value '01', with the key to be checked and retaining the 3 highest-order bytes of the encrypted result.

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0195

# C Secure Content Management

This appendix defines the different methods that shall be used to secure the changes and/or modifications to the content of a GlobalPlatform card. At this point in time, these methods are the only ones specified for GlobalPlatform cards. Depending on the implementation of the card, any subset of these methods may be supported.

## C.1 Keys

In order to perform the Card Content management operations described in the subsequent sub-sections different keys are required.

### C.1.1 Token and Receipt Keys

The Security Domain with Token Verification privilege and the Security Domain with Receipt Generation privilege shall have knowledge of different keys if Delegated Management is supported. These keys are used to secure the management of the card and its content.

| Key | Usage | Minimum Length | Remark |
|---|---|---|---|
| Token | Token verification (RSA Public Key) | 1024 bits | Delegated Management only |
| Receipt | Optional Receipt generation (DES) | 16 bytes | Delegated Management only |
| Receipt | Optional Receipt generation (RSA) | 1024 bits | Delegated Management only |

**Table C-1: Token and Receipt Keys**

It is recommended that RSA keys are a multiple of 32 bits in length above the minimum length.

#### C.1.1.1 Token key

If the card supports Delegated Management, the Security Domain with Token Verification privilege shall have an RSA Public Key to be used to verify a Token. Token verification and the corresponding delegated management operation shall fail if the Token verification key is not present.

#### C.1.1.2 Receipt Key

If the card supports Delegated Management and specifically Receipt generation, the Security Domain with Receipt Generation privilege shall either have an unambiguously recognized DES key or private RSA key to be used to generate Receipts. Receipt generation and the corresponding delegated management operation shall fail if the Receipt generation key is not present.

### C.1.2 DAP Verification Keys

If the Security Domain supports DAP Verification, the Security Domain shall have either an RSA public key or a DES key to verify Load File Data Block Signatures.

| Key | Usage | Minimum Length | Remark |
|---|---|---|---|
| DAP Verification | Load File Data Block Signature verification (RSA Public Key) | 1024 bits | DAP Verification only |

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0196

| Key | Usage | Minimum Length | Remark |
|---|---|---|---|
| DAP Verification | Load File Data Block Signature verification (DES Key) | 16 Bytes | DAP Verification only |

**Table C-2: Additional Security Domain Key**

It is recommended that RSA keys are a multiple of 32 bits in length above the minimum length.

## C.2 Load File Data Block Hash

The Load File Data Block Hash is a field that is required to be present in the INSTALL [for load] command if Delegated Management loading is occurring and/or the Load File contains one or more DAP Blocks. The purpose of this field is to provide a SHA-1 digest of the Load File Data Block and it is used to ensure that the contents of the Load File Data Block have not been modified in any way. While the actual hash is not secured in any manner, it is used in other secure operations that ensure that the Load File Data Block has not been modified and a new hash generated for the modified data. The OPEN shall verify the integrity of the Load File Data Block prior to creating an Executable Load File.

Figure C-1 details the Load File Data Block Hash calculation performed by the Security Domain, an Application Provider and a Controlling Authority.

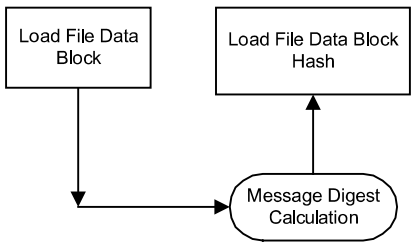



**Figure C-1: Load File Data Block Hash Calculation**

Padding of the data is as defined by the SHA-1. The digest is generated prior to the Load File Data Block being encapsulated in the TLV structure of the Load File (i.e. excluding tag 'C4' and its length).

When Delegated Management is occurring the Load Token is a signature of multiple fields including this hash and is proof that the Card Issuer generated the Token for the Load File Data Block linked to the hash.

If the Load File contains DAP Blocks, DAP Verification is the actual signing of this hash and is proof that the DAP Block was generated by an entity that verified the content of the Load File Data Block linked to the hash.

## C.3 Load File Data Block Signature (DAP Verification)

The Load File Data Block Signature provides verification of the Load File Data Block prior to commencing with the processing of the actual Load File Data Block. The OPEN shall request the Security Domain linked to the Load File Data Block Signature to verify the signature.

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0197

The Load File Data Block Signature is a signature of the Load File Data Block Hash. Each Load File Data Block Signature is combined with its linked Security Domain AID in the TLV structured DAP Block. DAP Blocks are positioned in the beginning of the Load File.

Figure C-2 details the Load File Data Block Signature calculation performed by an Application Provider or Controlling Authority.

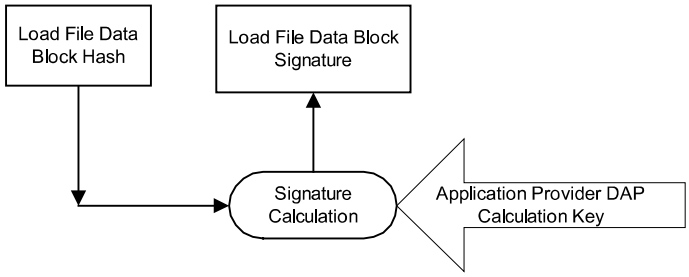



**Figure C-2: Load File Data Block Signature Calculation**

## C.4 Tokens

Tokens are public key signatures, used as proof that an Application Provider has been authorized to perform a Card Content Management operation. Tokens are generated and verified according to this appendix. Tokens may be generated for use on one or multiple cards.

The signature scheme for tokens is as defined in appendix B.3.

### C.4.1 Load Token

The Load Token is a signature authorizing the transmission of application code to the card. It allows for the verification of the load request. The OPEN shall request the Security Domain with Token Verification privilege to verify the Load Token.

The following figure shows the Load Token generation.

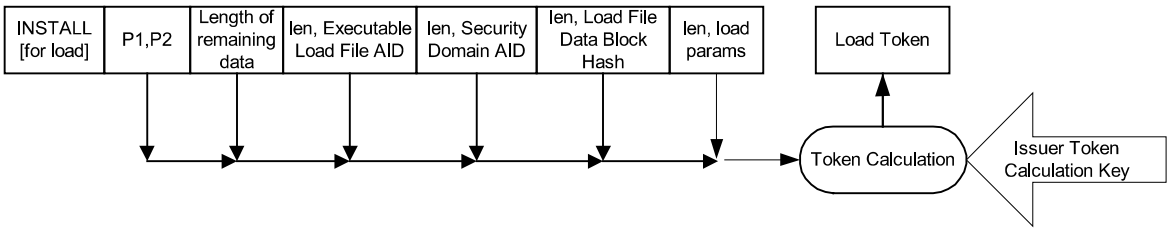



**Figure C-3 Load Token Calculation**

Generating a Load Token ensures the following:

- Only the application code (hash of the Load File Data Block) included in this signature may be loaded to the card;

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0198

- The AID of the Load File Data Block may only be that included in the signature;
- The Executable Load File (derived from the Load File Data Block) and all Executable Modules within the Executable Load File may only be associated with the Security Domain included in the signature;
- The issuer of the Load Token may only be the Security Domain Provider of the Security Domain with Token Verification Privilege.

The Load Token is an RSA signature of the following data that will be included in the actual INSTALL [for load] command to be transmitted to the card.

| Name | Length |
|---|---|
| Reference control parameter P1 | 1 |
| Reference control parameter P2 | 1 |
| Length of the following data fields (including the length fields) - see note below | 1 |
| Load File AID length | 1 |
| Load File AID | 5-16 |
| Security Domain AID length | 1 |
| Security Domain AID | 0 or 5-16 |
| Length of the Load File Data Block Hash | 1 |
| Load File Data Block Hash | 20 |
| Load parameters field length | 1-2 |
| Load parameters field | Var |

**Table C-3: Data Elements Included in the Load Token**

Note that 'Length of the following data fields' is the value of Lc of the INSTALL command, prior to a Token being added. It is coded on 1 byte with a value up to 255.

## C.4.2 Install Token

The Install Token allows for the verification of the installation process. The token is a signature authorizing the installation to the card of an Application (Executable Module) contained in a previously loaded file (Executable Load File). The OPEN shall request the Security Domain with Token Verification privilege to verify the Install Token.

Figure C-4 shows the Install Token generation.

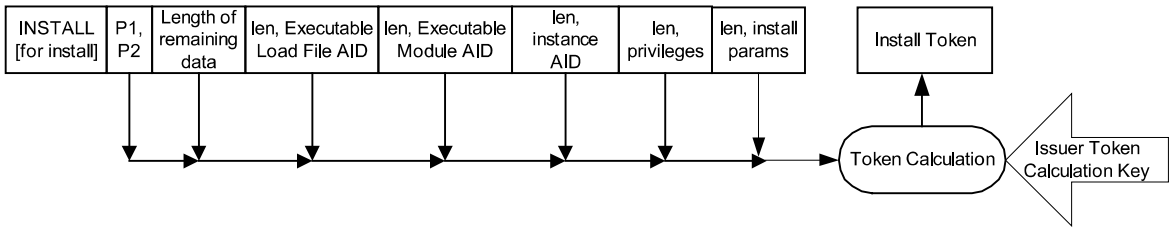



**Figure C-4: Install Token Calculation**

Generating an Install Token ensures the following:

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0199

- Only the application (Executable Module) included in this signature and present in the Executable Load File may be installed on the card;
- That only the instance AID included in this signature may be used as the AID to select the instance;
- The Application may only be installed with the privileges included in this signature;
- Only the parameters included in this signature may be used to install the Application;
- The issuer of the Install Token may only be the Security Domain Provider of the Security Domain with Token Verification Privilege.

The Install Token is an RSA signature of the following data that will be included in an INSTALL [for install] command.

| Name | Length |
|---|---|
| Reference control parameter P1 | 1 |
| Reference control parameter P2 | 1 |
| Length of the following data fields (including the length fields) - see note below | 1 |
| Executable Load File AID length | 1 |
| Executable Load File AID | 5-16 |
| Executable Module AID length | 1 |
| AID within the Executable Load File | 5-16 |
| Instance AID length | 1 |
| Instance AID | 5-16 |
| Privileges length | 1 |
| Privileges (byte 1 - byte 2 – byte 3) | 1 or 3 |
| Install Parameters field length | 1-2 |
| Install Parameters (system and Application) field | Var |

**Table C-4: Data Elements Included in the Install Token**

Note that 'Length of the following data fields' is the value of Lc of the INSTALL command, prior to a Token being added. It is coded on 1 byte with a value up to 255.

### C.4.3 Make Selectable Token

The Make Selectable Token allows for the verification of the installation for make selectable process. The token is a signature authorizing the making selectable of an Application. The OPEN shall request the Security Domain with Token Verification privilege to verify the Make Selectable Token.

The following figure shows the Make Selectable Token generation.

*Copyright © 2006-2011 GlobalPlatform Inc. All Rights Reserved.*
*The technology provided or described herein is subject to updates, revisions, and extensions by GlobalPlatform. Use of this information is governed by the GlobalPlatform license agreement and any use inconsistent with that agreement is strictly prohibited.*

Petitioner Samsung Ex-1006, 0200