BC Services Card Project

IAS and CMS
Interface Design Specification

Version: 1.2 Final
May 29, 2012

Document Information

This is a point-in-time version of a document. Please contact the author or the person who issued this document (listed below) if you are in any doubt about the currency of this document.

Document title	IAS and CMS Interface Design Specification
Document filename	BCSC_IAS_CMS_Interface_Design_Specification_v1_2_final
Revision number	1.2 Final
Issued by	Eli Erlikhman (eli.erlikhman@securekey.com)
Issue Date	May 29, 2012
Status	Final

Document Purpose and Intended Audience

This document describes the design details of the information exchanges between BC's Identity Assurance Services (IAS) and SecureKey's Card Management Service (CMS) to support the card issuance and management functions of the BC Services Card program.

This scope of this design is slightly broader than the set of interfaces due to be put into production operations on November 30th, 2012. For example, an interface is defined for putting a card on hold, however this will not be implemented immediately. The goal is to define a reasonably complete set of interfaces so as to minimize re-design later.

This document is intended for the designers of the IAS and CMS to agree on the design specification, and for the test leads of the IAS and CMS to determine the test cases.

Document Approvals

Name, Title	Signature	Date
Ian Bailey ED Architecture & Standards and A/CISO, Office of the CIO, LCTZ, Province of BC	*IB* *Approved by email*	Jun 1, 2012
Dmitry Barinov Chief Architect, CSO SecureKey Technologies, Inc.	*DB* *Approved by email*	May 31, 2012

Document Reviewers

Representing Province of BC	Representing SecureKey
Patricia Wiebe Director and Solution Architect Office of the CIO, LCTZ	Eli Erlikhman Director Security Architecture SecureKey Technologies, Inc
Greg Turner Technical Architect Sierra Systems, Inc	Ayinde Yakubu Solution Architect SecureKey Technologies, Inc
Marcos Carretero Technical Designer on behalf of Sierra Systems, Inc	Maggie Au Professional Services SecureKey Technologies, Inc
Steve Shulhan (Reporting section) Solution Architect IDIM Program, LCTZ	Chris Chapman Project Delivery Manager SecureKey Technologies, Inc

Document Version History

Version	Date	Author	Summary of Changes
0.1 to 0.8	Apr 8, 2012 to Apr 16, 2012	Patricia Wiebe, Maggie Au, Ayinde Yakubu	Drafts based on draft technical design documents, emails, notes, discussions and contract SOW
1.0	Apr 17, 2012	Patricia Wiebe	Issued final draft
1.1	May 27, 2012	Eli Erlikhman	Updated the final draft to clarify security requirements and how MAC field will be used. Added an Appendix to contain the details of the security design
1.2	May 29, 2012	Eli Erlikhman	Updated based on Patricia's feedback on version 1.1 and changes to document approvers

Document Contents

Figures

Tables

1. SOLUTION CONTEXT

This section of the document describes the high level business processes and solution architecture related to the BC Services Card program that are in scope for the issuance and management of cards that is in scope for the November 30, 2012 release.

1.1. Card Manufacturing

The following diagram illustrates the high level business process of ordering, manufacturing and receiving card stock to support the next business process of issuing cards.

Figure 1: High Level Card Manufacturing Process

This diagram is provided for context, but does not have interfaces that are in scope of the IAS-CMS system integration. It is important to note that CMS generates chip personalization data for IRIS and then is notified by IRIS about chips that are personalized so that CMS can manage the early card states of a PAN. See also section 3.2.1, “PAN States within CMS”.

1.2. Card Issuance

The following diagram illustrates the high level business process of requesting, producing, notifying other parties, and mailing a card to the client. The highlighted area represents several interactions between IAS and CMS systems that will be further described in this document.

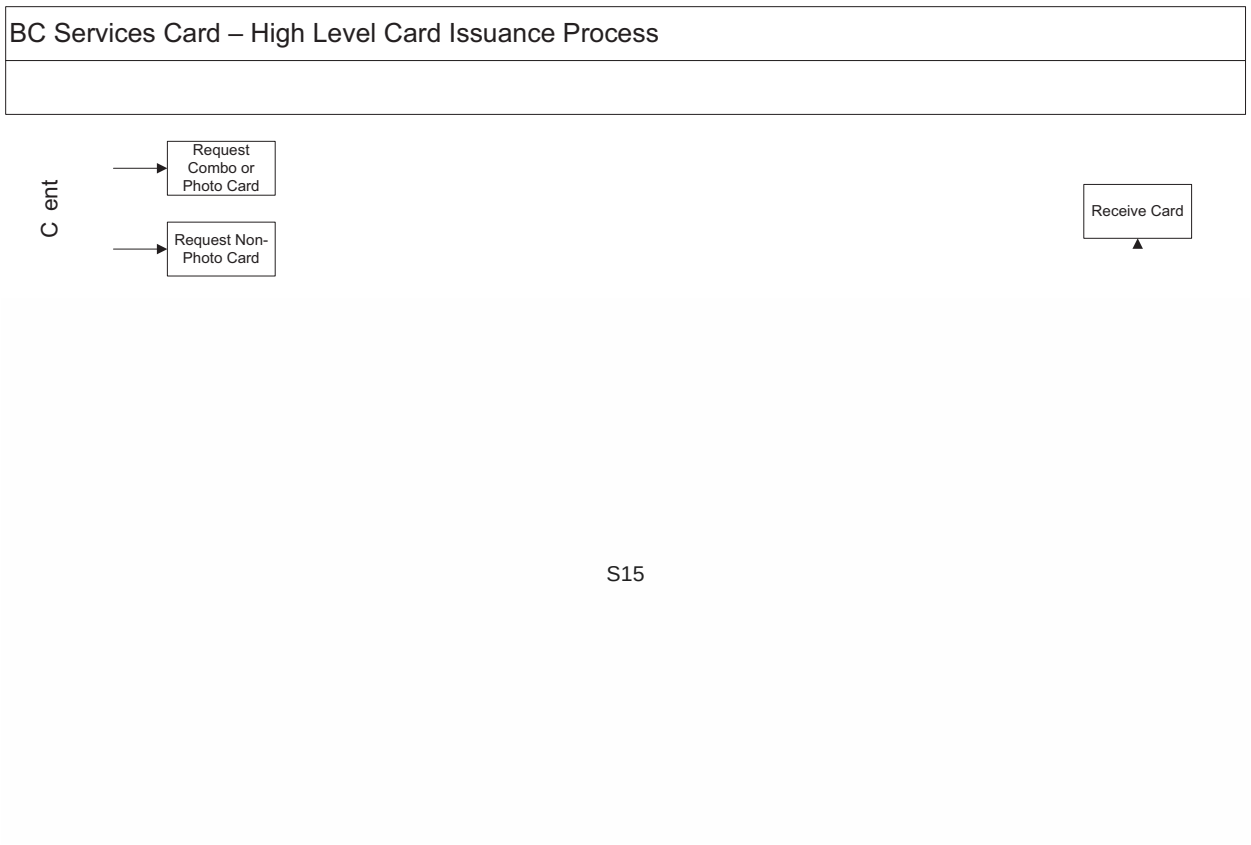


Figure 2: High Level Card Issuance Process

The following is a list of specific interactions relevant to this business process between IAS and CMS systems:

a) IAS provides CMS with a list of cards to be activated in CMS. The detailed design of this interaction is provided in section 2.1, “Activate PANs”.

b) IAS provides CMS with a list of cards that were spoiled during card production to be deactivated in CMS. The detailed design of this interaction is provided in section 2.2, “Deactivate PANs”.

c) CMS responds to IAS with a confirmation of card status updates processed. The detailed design of this interaction if provided in section 2.5, “Confirmation of Card Status Updates”.

1.3. Card Lifecycle Management

The following diagram illustrates the high level business process of cancelling, expiring and suspending cards. The highlighted area represents an interaction between IAS and CMS systems that will be further described in this document.

There may be various business reasons to cancel a card, but the end result is that the card is deactivated. Similarly, there may be various business reasons to suspend, however this does not cancel a card; the card can be unsuspended and resumed to its active state. The only business reason to expire is that the card is past the expiry date printed on the card.

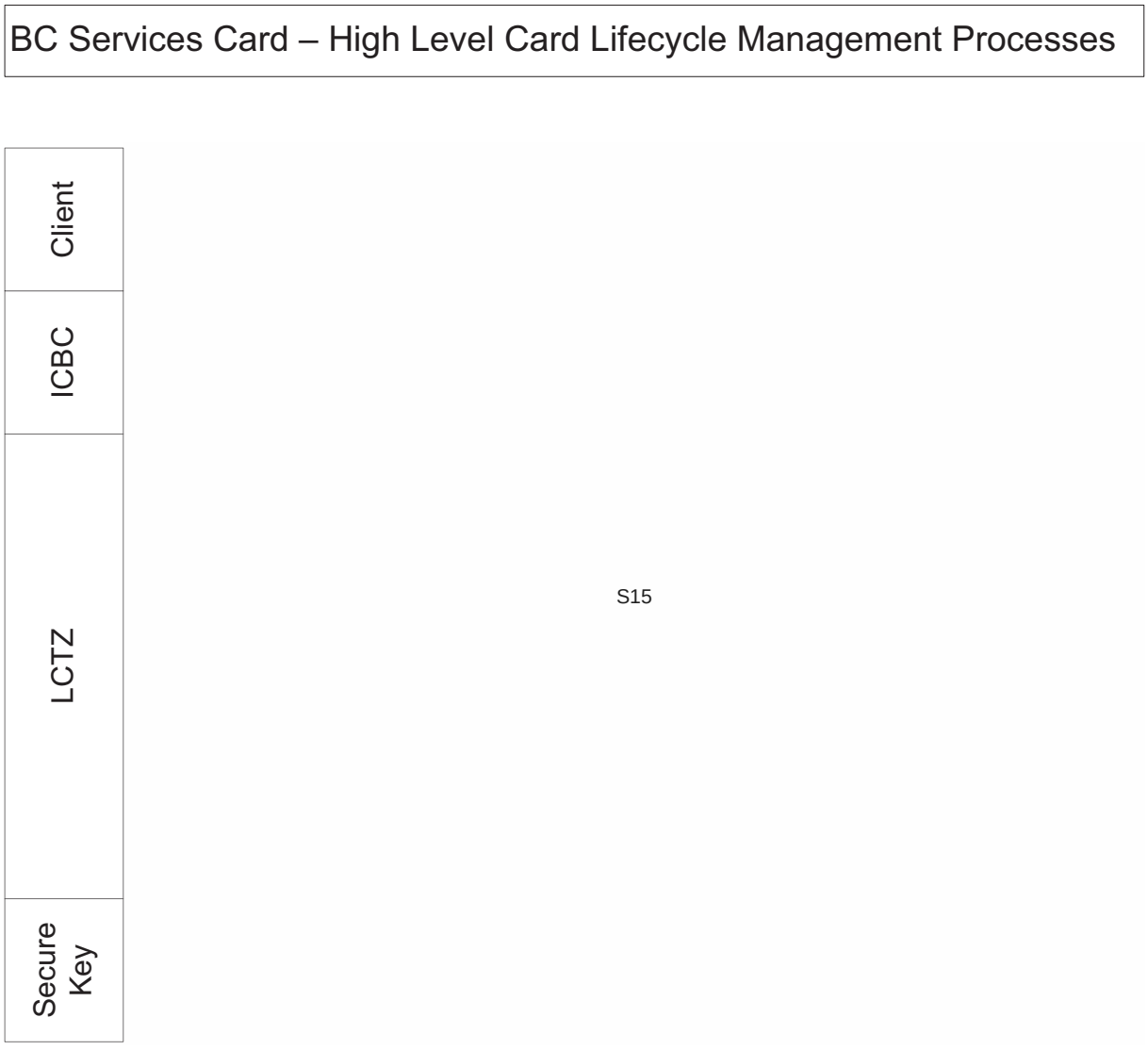


Figure 3: High Level Card Lifecycle Management Processes

The following is a list of specific interactions relevant to this business process between IAS and CMS systems:

a) IAS provides CMS with a list of cards that were cancelled for various business reasons after the cards were issued, to be deactivated in CMS. The detailed design of this interaction is provided in section 2.3, “Deactivate MBUNs”.

b) IAS provides CMS with a list of cards that have expired after the cards were issued to be deactivated in CMS. The detailed design of this interaction is combined with the above one in section 2.3, “Deactivate MBUNs”.

c) IAS provides CMS with a list of cards that are to be suspended for various business reasons after the cards were issued, to be put “on hold” in CMS. The detailed design of this interaction is provided in section 2.4, “Suspend/Unsuspend MBUNs”.

d) IAS provides CMS with a list of cards that are to be unsuspended, to be put back into an active state in CMS. The detailed design of this interaction is combined with the above one in section 2.4, “Suspend/Unsuspend MBUNs”.

e) CMS responds to IAS with a confirmation of card status updates processed. The detailed design of this interaction if provided in section 2.5, “Confirmation of Card Status Updates”.

1.4. Operational Reporting

The following diagram illustrates the high level business process of operational reporting, though is focused only on LCTZ and SecureKey. There will be other operational reporting across the partner organizations. The highlighted area represents an interaction between IAS and CMS systems that will be further described in this document. The interaction for the resolution of issues is not proposed to be a system interaction and will be described in a subsequent operational procedures document.

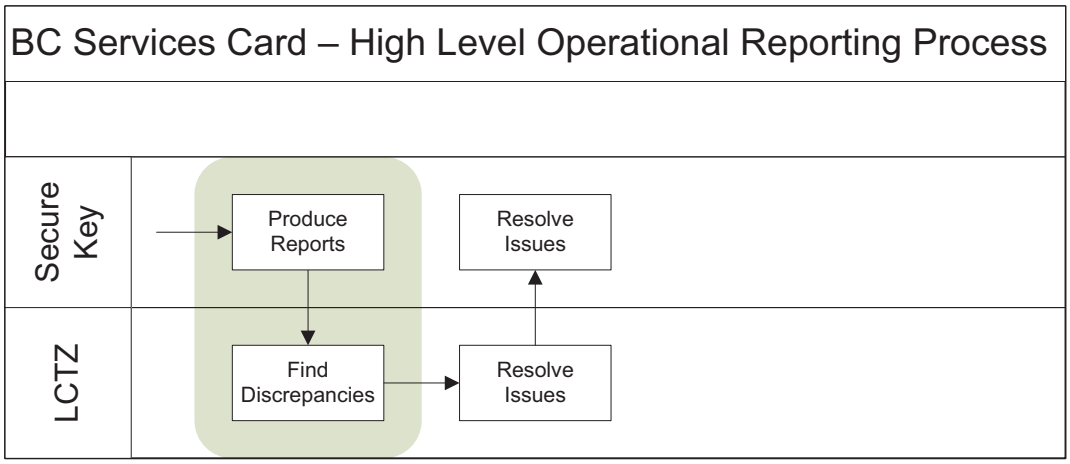


Figure 4: High Level Operational Reporting Process

The following is a list of specific interactions relevant to this business process between IAS and CMS systems:

a) CMS provides IAS with an operational report of card status updates that were processed by CMS over the past week in the production operational environment. The detailed design of this interaction is provided in section 2.6, “Report of Card Status Updates”.

b) CMS provides IAS with an operational report of CMS service outages and restores that occurred over the past week in the production operational environment. The detailed design of this interaction is provided in section 2.7, “Report of Service Restores”.

c) CMS provides IAS with an operational report of the operational support performed by SecureKey operational support staff over the past week related to the production operational environment. The detailed design of this interaction is provided in section 2.8, “Report of Operational Support”.

1.5. Solution Architecture

The following diagram illustrates the high level solution architecture related to the processes of card manufacturing and card issuance. The diagram is a simplified view of many information exchanges between the partners organizations involved in the BC Services Card program.

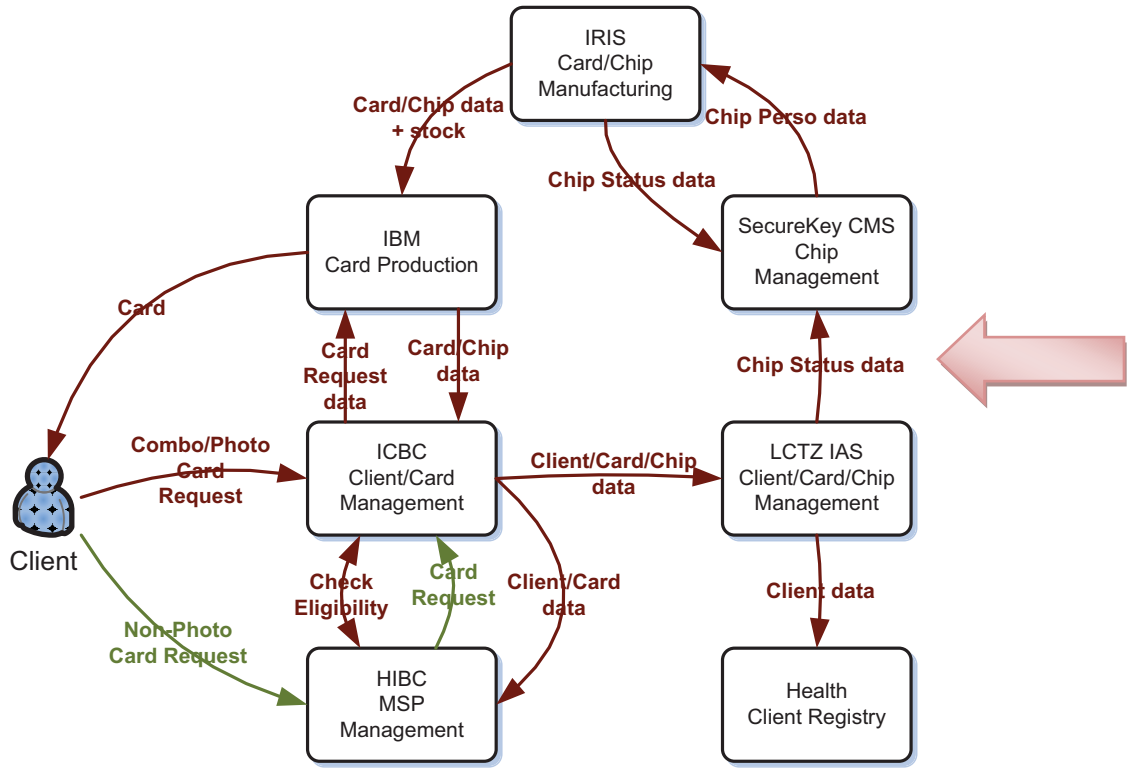


Figure 5: High Level Solution Architecture

The top half of the diagram illustrates the information exchanges between SecureKey, IRIS that IBM support the high level card manufacturing business process described in section 1.1.

The bottom half of the diagram illustrates the information exchanges between ICBC, IBM and HIBC that support the high level card issuance business process described in section 1.2. After a card is produced, HIBC and LCTZ are notified at the same time as the card is put in the mail to be sent to the client. The final information exchanges are related to LCTZ updating SecureKey with card statuses, and LCTZ updating the health registry of the client information that was printed on the card.

The diagram does not specifically illustrate the information exchanges between ICBC and LCTZ that support the high level card lifecycle management processes described in section 1.3, but the flows are similar to that of card issuance.

The focus of this design document is the information exchanges between LCTZ's IAS and SecureKey's CMS systems, where the arrow is pointing.

2. INTERFACES

This section of the document describes the detailed design of the interactions between IAS and CMS mentioned in the high level business processes related to the BC Services Card program that are in scope for the issuance and management of cards.

2.1. Activate PANs

In this interface, IAS provides CMS with a list of cards to be activated in CMS.

2.1.1. Flow of Activate PANs

The flow of steps is illustrated in the following diagram, starting with the notification about card production to IAS from ICBC for context purposes. This diagram illustrates the 3 types of card status update that will be provided by ICBC to IAS:

a) cards that are issued, and need to be registered in IAS and activated in CMS (described on the next page);

b) cards that were spoiled during card production, and need to be deactivated in CMS (described in section 2.2); and,

c) cards that were cancelled after card issuance, and need to be cancelled in IAS and deactivated in CMS (described in section 2.3).

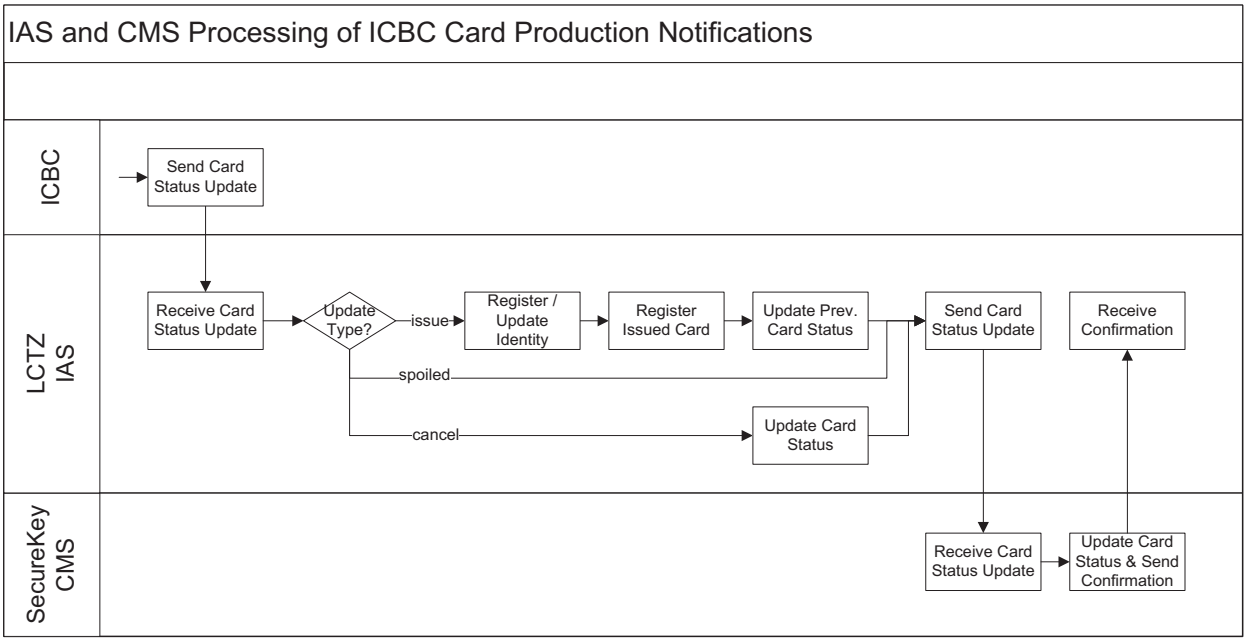


Figure 6: IAS and CMS Processing of ICBC Card Production Notifications

2.1.2. Data Elements of Activate PANs

The activation list will be communicated using records in XML format, described in Appendix C "File Structures", and exchanged using the SFTP communication pattern described in section 4.1.

The data elements that are included in the activation list are provided in the following table. The detailed schema is also provided in Appendix C.

Table 1: Data Elements of Activate PANs

#	Data Element Name	Description	Data Format & Rules	Cross reference to XML schema
1.	Record Number	An index of records within a file. Records will be processed in numeric ascending order.	Required Integer	
2.	EPAN	The encrypted value of PAN-SN, encrypted by the card producer (IBM) for CMS to decrypt.	Required String, 256 chars	
3.	MBUN	The Meaningless But Unique Number associated with the PAN, as assigned by IAS.	Required String	S 15
4.	Card Expiry Date	The expiry date of the issued card, as engraved on the card.	Required Date	
5.	Card Issue Request Type	An indicator of whether CMS should interpret this card as new or replacement for a cardholder.	Required String, code list: "NEW" or "REPLACE"	

2.2. Deactivate PANs

In this interface, IAS provides CMS with a list of cards that were spoiled during card production to be deactivated in CMS.

2.2.1. Flow of Deactivate PANs

The flow of steps is illustrated in the above diagram in section 2.1.1.

2.2.2. Data Elements of Deactivate PANs

The deactivation list will be communicated using records in XML format, described in Appendix C, and exchanged using the SFTP communication pattern described in section 4.1.

The data elements that are included in the deactivation list are provided in the following table. The detailed schema is also provided in Appendix C.

Table 2: Data Elements of Deactivate PANs

#	Data Element Name	Description	Data Format & Rules	Cross reference to XML schema
1.	Record Number	An index of records within a file. Records will be processed in numeric ascending order.	Required Integer	S 15
2.	EPAN	The encrypted value of PAN-SN, encrypted by the card producer (IBM) for CMS to decrypt.	Required String, 256 chars	
3.	Deactivation Reason	An indicator of why the card is being deactivated.	Required String, code list: “SPOILED”	

2.3. Deactivate MBUNs

In this interface, IAS provides CMS with a list of cards that were cancelled for business reasons or expired after card issuance to be deactivated in CMS.

2.3.1. Flow of Deactivate MBUNs

The flow of steps related to ICBC cancelling a card is illustrated in the above diagram in section 2.1.1. The flow of steps related to IAS affecting change a card status is illustrated in the following diagram. This diagram illustrates 4 types of card status updates that could occur within IAS:

a) cards that are cancelled in IAS and need to be deactivated in CMS (described on the next page);

b) cards that are expired in IAS and need to be deactivated in CMS (described on the next page);

c) cards that are suspended in IAS and need to be put on hold (but not deactivated) in CMS (described in section 2.4Suspend/Unsuspend MBUNs); and,

d) cards that are unsuspended in IAS and need to be put back into active state in CMS (described in section 2.4Suspend/Unsuspend MBUNs).

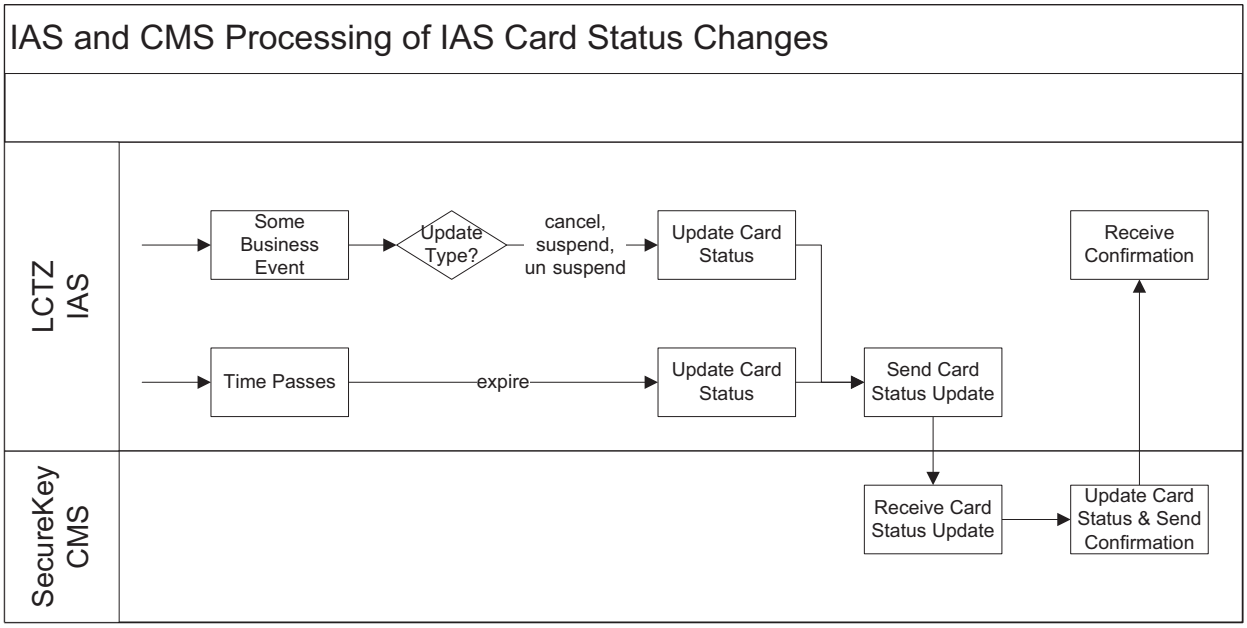


Figure 7: IAS and CMS Processing of ICBC Card Status Changes

2.3.2. Data Elements of Deactivate MBUNs

The deactivation list will be communicated using records in XML format, described in Appendix C, and exchanged using the SFTP communication pattern described in section 4.1.

The data elements that are included in the deactivation list are provided in the following table. The detailed schema is also provided in Appendix C.

Table 3: Data Elements of Deactivate MBUNs

#	Data Element Name	Description	Data Format & Rules	Cross reference to XML schema
1.	Record Number	An index of records within a file. Records will be processed in numeric ascending order.	Required Integer	
2.	MBUN	The Meaningless But Unique Number associated with the PAN, as assigned by IAS.	Required String	S 15
3.	Deactivation Reason	An indicator of why the card is being deactivated.	Required String, codelist: “CANCELLED” or “EXPIRED”	

2.4. Suspend/Unsuspend MBUNs

In this interface, IAS provides CMS with a list of cards that were suspended for business reasons after card issuance to be put “on hold” in CMS. This same interface can be used to unsuspend cards and put the cards back into active state in CMS.

2.4.1. Flow of Suspend/Suspend MBUNs

The flow of steps is illustrated in the above diagram in section 2.3.1.

2.4.2. Data Elements of Suspend/Unsuspend MBUNs

The deactivation list will be communicated using records in XML format, described in Appendix C, and exchanged using the SFTP communication pattern described in section 4.1.

The data elements that are included in the deactivation list are provided in the following table. The detailed schema is also provided in Appendix C.

Table 4: Data Elements of Suspend/Unsuspend MBUNs

#	Data Element Name	Description	Data Format & Rules	Cross reference to XML schema
1.	Record Number	An index of records within a file. Records will be processed in numeric ascending order.	Required Integer	
2.	MBUN	The Meaningless But Unique Number associated with the PAN, as assigned by IAS.	Required String	S 15
3.	Hold Request Type	An indicator of what to do with the card status.	Required String, codelist: “HOLD” or “RELEASE”	

2.5. Confirmation of Card Status Updates

In this interface, CMS provides IAS with a confirmation of the card status updates that it processed from all of the files that CMS received that day.

2.5.1. Flow of Confirmation of Card Status Updates

The flow of steps is illustrated in both of the above diagrams in sections 2.1.1 and 2.3.1.

2.5.2. Data Elements of Confirmation of Card Status Updates

The data elements that are included in the confirmation are provided in the following table. The detailed schema is provided in Appendix C. A confirmation file is provided corresponding to each list provided by IAS to CMS.

Table 5: Data Elements of Confirmation of Card Status Updates

#	Data Element Name	Description	Data Format & Rules	Cross reference to XML schema
1.	File Name	The name of the referenced file of card status updates.	Required String	
2.	File Schema Version	The version number indicated in the referenced file.	Required String	
3.	File Timestamp	The timestamp indicated in the referenced file.	Required Date & Time (including an offset from the UTC time by adding a positive or negative time behind the date)	
4.	File Author	The name of the organization indicated in the referenced file.	Required String	
5.	File Record Count	The count of all records processed in referenced file.	Required Integer	S 15
6.	Comments	The description in the referenced file.	Optional String	
6.	Signature Value	This field will be used as one of the parameters by LCTZ to map confirmation files to request files. The value of Signature Value field will be populated by SecureKey as per Appendix D – Security Design.	Required String	
7.	File Size	The size of the reference file that can be used to validate data integrity of the exchange.	Required Long Measured in bytes	

8.	Processing Status	The result of the processing of the referenced file.	Required String, codelist: “SUCCEEDED” or “FAILED”	
9.	Processing Start Time	The timestamp of when CMS started processing the file.	Required Date & Time (including an offset from the UTC time by adding a positive or negative time behind the date)	S 15
10.	Processing End Time	The timestamp of when CMS finished processing the file.	Required Date & Time (including an offset from the UTC time by adding a positive or negative time behind the date)	

Where the Processing Status is “FAILED”, (i.e. there were errors encountered during processing), there will be additional data elements in the file. If there are multiple errors for a given record, there will be multiple sets of data elements, one per error, as described in the following table.

#	Data Element Name	Description	Data Format & Rules	Cross reference to XML schema
11.	Error Code	An indicator of the type of error found in a record.	Required if error reported; String	
12.	Error Record Number	A reference to the record that had an error.	Optional if error reported; Long	
13.	Error Severity	An indicator of the severity of the error found in a record.	Required if error reported; String, codelist: “CRITICAL”, “MAJOR”, “MINOR”, “COSMETIC”	S 15
14.	Error Description	A description that corresponds with the error code provided.	Required if error reported; String	

2.6. Report of Card Status Updates

In this interface, IAS provides CMS with an operational report of card status updates that were processed by CMS over the past week in the production operational environment.

2.6.1. Flow of Report of Card Status Updates

The flow of steps is illustrated in the following diagram. Resolution of discrepancies or other issues will be a manual operational procedure and is not described in this document.

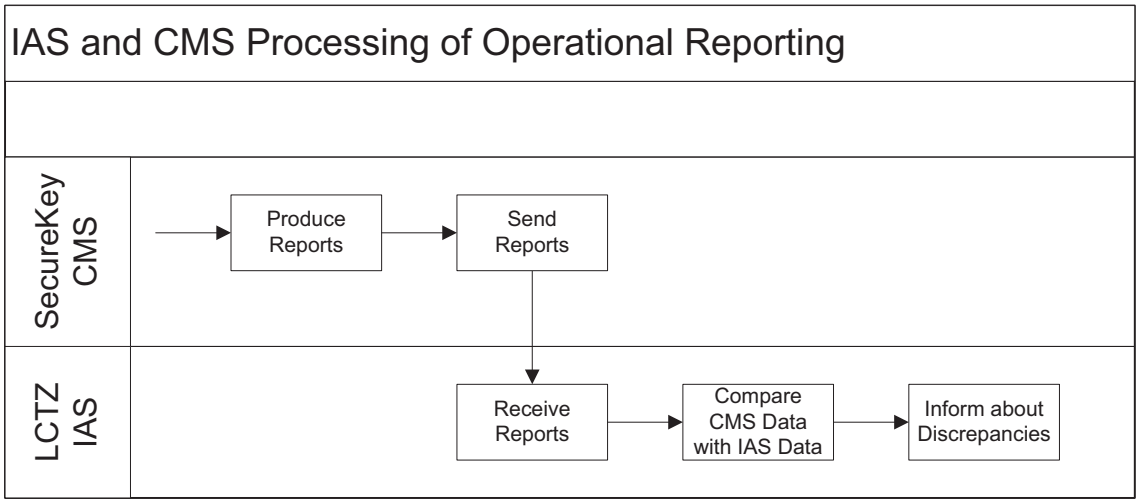


Figure 8: IAS and CMS Processing of Operational Reporting

2.6.2. Data Elements of Report of Card Status Updates

The operational report will be communicated using records in XML format, described in section 1.4, and exchanged weekly on a Wednesday, using the SFTP communication pattern described in section 4.1. Reporting periods are expected to be Sunday to Saturday, Pacific time zone.

The data elements that are included in the report are provided in the following table. The detailed schema is provided in Appendix C.

Table 6: Data Elements of Report of Card Status Updates

#	Data Element Name	Description	Data Format & Rules	Cross reference to XML schema
1.	Report Start	The date and time indicating the start of the reporting period.	Required Date & Time Should be Sunday 00:00:00 (including an offset from the UTC time by adding a positive or negative time behind the date)	S 15

2.	Report End	The date and time indicating the end of the reporting period.	Required Date & Time Should be Saturday 23:59:59 (including an offset from the UTC time by adding a positive or negative time behind the date)	
3.	Record Number	An index of records within a file. Records will be processed in numeric ascending order.	Required Integer	
4.	Card Status Request Type	An indicator of what card status update was requested to be processed.	Required String, codelist: “NEW”, “REPLACE”, “SPOILED”, “CANCELLED”, “EXPIRED”, “HOLD”, “RELEASE”	S 15
5.	Record Success Count	The count of all records successfully processed, filtered by a given card status request type. This count is the sum across all files processed during the reporting period.	Required Integer	
6.	Record Error Count	The count of all records that were found with (one or more) errors within a record, filtered by a given card status request type. This count is the sum across all files processed during the reporting period. The error count should reflect what was originally detected, regardless of whether or not the records were subsequently resolved.	Required Integer	

7.	File Error Count	The count of all files that were found with (one or more) errors within the file, filtered by a given card status request type. This count is the sum of all files with errors processed during the reporting period, regardless of whether or not the files were subsequently resolved.	Required Integer	S 15

This data file could be presented visually to an operations staff person like this:

```
Report Start Date:  2012 02 05T12:00:00 08:00
Report End Date:  2012 02 11T11:59:59 08:00
```

Card Status Request Type	Record Success Count	Record Error Count	File Error Count
NEW	24497	3	1
REPLACE	499	1	0
SPOILED	9	0	0
CANCELLED	12	3	0
EXPIRED	5	0	0
HOLD	2	0	0
RELEASE	3	1	1

```
Total activations: 25000
      Total new: 24500
      Total replace: 500
Total deactivations: 29
      Total spoiled: 9
      Total cancelled: 15
      Total expired: 5
Total suspends/unsuspends: 6
      Total holds: 2
      Total releases: 4

Total file errors: 2
```

Note: Activations of type REPLACE will lead to a transition of an MBUN and deactivation of the previous PAN. This count must not be included in the deactivation count.

Also, Deactivations of type DAMAGED are from IRIS, and must not be included in the deactivation count.

When there is a file that is unreadable, it is represented in the file error count. If it was subsequently corrected during the same reporting period, its records would be included in the success and error counts.

2.7. Report of Service Restores

In this interface, SecureKey provides IAS with an operational report of service outages and restores over the past week in the production operational environment. Note that this section is not finalized, and is provided as a draft only; it is a starting point for subsequent discussions on operational management.

2.7.1. Flow of Report of Service Restores

The flow of steps about exchanging reports in general is illustrated in the above diagram in section 2.6.1.

2.7.2. Data Elements of Report of Service Restores

The operational report will be communicated using records in XML format, described in section 1.4, and exchanged weekly on a Wednesday, using the SFTP communication pattern described in section 4.1. Reporting periods are expected to be Sunday to Saturday, Pacific time zone.

The data elements that are included in the report are provided in the following table. The detailed schema is provided in Appendix C.

Table 7: Data Elements of Report of Service Restores

#	Data Element Name	Description	Data Format & Rules	Cross reference to XML schema
1.	Report Start	The date and time indicating the start of the reporting period.	Required Date & Time Should be Sunday 00:00:00 (including an offset from the UTC time by adding a positive or negative time behind the date)	not yet defined
2.	Report End	The date and time indicating the end of the reporting period.	Required Date & Time Should be Saturday 23:59:59 (including an offset from the UTC time by adding a positive or negative time behind the date)	not yet defined
3.	Event Identifier	An identifier that represents the service outage event.	Required String	not yet defined
4.	Event Start	The date and time indicating the start of the service outage.	Required Date & Time	not yet defined

5.	Event End	The date and time indicating the end of the service outage, i.e. when the service was restored.	Required Date & Time	not yet defined
6.	Restore Type	An indicator of the type of activity performed on the service to return it to service.	Required String, codelist: Not yet defined	not yet defined
7.	Priority Level	An indicator of the significance and severity of the service outage, as defined in the contract.	Required String, codelist: P1, P2, P3, P4	not yet defined
8.	Service Type	An indicator of the type of service that had the outage and was restored.	Required String, codelist: Not yet defined (CMS vs Authn vs other)	not yet defined

2.8. Report of Operational Support

In this interface, SecureKey provides IAS with an operational report of the operational support performed by SecureKey (Tier 3) support staff over the past week in the (production) operational environment. Note that this section is not finalized, and is provided as a draft only; it is a starting point for subsequent discussions on operational management.

2.8.1. Flow of Report of Operational Support

The flow of steps about exchanging reports in general is illustrated in the above diagram in section 2.6.1.

2.8.2. Data Elements of Report of Operational Support

The operational report will be communicated using records in XML format, described in section 1.4, and exchanged weekly on a Wednesday, using the SFTP communication pattern described in section 4.1. Reporting periods are expected to be Sunday to Saturday, Pacific time zone.

The data elements that are included in the report are provided in the following table. The detailed schema is provided in Appendix C.

Table 8: Data Elements of Report of Operational Support

#	Data Element Name	Description	Data Format & Rules	Cross reference to XML schema
1.	Report Start	The date and time indicating the start of the reporting period.	Required Date & Time Should be Sunday 00:00:00 (including an offset from the UTC time by adding a positive or negative time behind the date)	not yet defined
2.	Report End	The date and time indicating the end of the reporting period.	Required Date & Time Should be Saturday 23:59:59 (including an offset from the UTC time by adding a positive or negative time behind the date)	not yet defined
3.	Event Identifier	An identifier that represents the operational incident event.	Required String	not yet defined
4.	Event Start	The date and time indicating the start of the support event.	Required Date & Time	not yet defined
5.	Event End	The date and time indicating the end of the support event.	Required Date & Time	not yet defined

6.	Support Type	An indicator of the type of activity performed to support the service.	Required String, codelist: Not yet defined	not yet defined
7.	Priority Level	An indicator of the significance and severity of the incident or other requirement to require the tier 3 support effort, as defined in the contract.	Required String, codelist: P1, P2, P3, P4	not yet defined
8.	Service Type	An indicator of the type of service that was related to the operational support.	Required String, codelist: Not yet defined (CMS vs Authn vs other)	not yet defined

3. INTERNAL PROCESSING

This section of the document describes the detailed design of the processing internal to each of IAS and CMS in reference to the interfaces in the previous section related to the BC Services Card program that are in scope for the issuance and management of cards.

3.1. Business Rules Relevant to IAS and CMS

CMS and IAS both manage cards and their states relevant to card issuance and lifecycle management. CMS manages data about all cards (emphasis on chips) to support future authentication of the cards with SecureKey card readers and the SecureKey authentication service. IAS manages data about identities, issued cards (and chips), to support future information sharing of identity information, generally with authentication of the cards.

The following table lists relevant business rules in the IAS that is relevant to the management of cards and their states within IAS and CMS.

Table 9: Business Rules about Card Issuance and Management

#	Business Rules	Implication to IAS and CMS
1.	A client is only allowed to have one active (or in use) card at a time; there is one exception that a child in a split family may request a second active non-photo card.	A client will have one MBUN assigned to a card and it's PAN; for the exception, a child with two cards will have two MBUNs. When the IAS detects an existing active card, it will consider an issued card as a replacement or renewal. After IAS and CMS processing, the previous active card will not be usable for authentication.
2.	A card may be used for authentication as soon as it is issued to a client.	A card must be issued to a client in a usable state. After a card is produced the IAS and CMS must be notified so that it can activate the card to prepare for an authentication event.
3.	A combo or photo card is associated with identification level 3, and a non-photo is associated with identification level 1.	An identity in IAS will be marked with an identification level, and a card in IAS will be marked with a card type. The CMS will not distinguish between card types or identification levels.

4.	A card may be active in the hands of the client for a range of 6 months to 5 years 6 months. A client with a temporary identity document (e.g. student visa) has a card expiry date that aligns with the temporary identity document expiry date. Generally a client has a card for two or five years. The card expiry date once set should not be changed.	The IAS and CMS must allow for a range of card expiry dates. The IAS will notify CMS to deactivate a card on the card expiry date. The CMS will also be notified of the card expiry date for informational and planning purposes when a card is issued. The CMS should not deactivate a card on its card expiry date without being notified by IAS.
5.	A client may request a replacement to their card when they claim it was lost, stolen, seized, defective or damaged; or when the client requests to change their name or gender (with supporting documentation). A replacement is allowed during the time after a card is issued and up to 6 months before the card expiry date. A replacement becomes a renewal if within 6 months of the card expiry date.	The IAS will detect when a card is being replaced, and notify the CMS of this ("REPLACE"). The IAS will transition the client's passcode and preferences from the previous card to the new card. The CMS will transition the client's authentication preferences and mobile devices from the previous card to the new card. After IAS and CMS processing, the previous active card will not be usable for authentication. IAS and CMS must not change the status of the previous card back to active.
6.	A client should request to renew their card before their current card expires; a renewal is allowed up to 6 months before the card expiry date.	The IAS will detect when a card is being renewed, and notify the CMS of this as if it were a replacement ("REPLACE"). The IAS will transition the client's passcode and preferences from the previous card to the new card. The CMS will transition the client's authentication preferences and mobile devices from the previous card to the new card. After IAS and CMS processing, the previous active card will not be usable for authentication. If a client does not request to renew before expiry, when the IAS is notified of a new card issued to a client, the IAS will generate a new MBUN and notify the CMS of this ("NEW").
7.	When a card expires, it can no longer be used for authentication.	After a card reaches the expiry date printed on the card, the IAS and CMS must be notified so that it can deactivate the card and fail an authentication event. After a card is expired, IAS and CMS must not change the status of the card back to active.

8.	A card may be cancelled for various business reasons by ICBC or LCTZ. When a card is cancelled, it can no longer be used for authentication.	After a card is cancelled the IAS and CMS must be notified so that they can deactivate the card and fail an authentication event. After a card is cancelled, IAS and CMS must not change the status of the card back to active.
9.	A card may be suspended for various business reasons by LCTZ. When a card is suspended, it can no longer be used for authentication.	After a card is suspended the IAS and CMS must be notified so that it can suspend and put “on hold” the card and fail an authentication event. A card may also be cancelled or expired from the suspended state.
10.	A card may be unsuspended for various business reasons by LCTZ. When a card is unsuspended, it can be used for authentication again.	After a card is suspended the IAS and CMS must be notified so that it can unsuspend and release the hold on the card and pass an authentication event.
11.	A card is generally issued to a client through postal mail, however a client may request to pick up their card in person at an ICBC counter. Returned mail for combo and photo cards is held by ICBC; on a monthly basis an updated address is looked for, and if found the mail is resent. Returned mail for non-photo cards is held by HIBC (do not know the rules for holding and resending).	When a card is returned, IAS and CMS should be notified so that it can suspend and put “on hold” the card and fail an authentication event. When a card is resent, IAS and CMS should be notified so that it can unsuspend and release the hold on the card and pass an authentication event.

3.2. Card States within CMS and IAS

CMS and IAS both manage card states. CMS manages the entire lifecycle of the card from the initial activity of preparing the chip personalization data before the card is manufactured to the final activities that end the use of the card. IAS manages a subset of that lifecycle, from the initial activity of issuing the card to the final activities that end the use of the card. Both systems need to keep in synch with each other; IAS is the authority on card state changes after it has been issued (activated) and will inform CMS of every card state change.

Note that there are two states “ACTIVE” and “IN USE” for a card. The former represents when a card has been issued to a client and is assumed to be in the hands of the client but has not yet been used. The latter represents when a card has started to be used in authentication transactions, and will be significant to the invoicing between LCTZ and SecureKey. Generally the first use of a card in an authentication transaction will trigger this state change, however there may be exceptions to this based on the type of authentication transaction, e.g. for changing a passcode associated with a card. This will be further defined in a separate design document about the authentication interfaces between LCTZ and SecureKey.

3.2.1. PAN States within CMS

CMS manages the card state using PAN as the primary identifier. The following diagram shows the set of states of a PAN (representing a card) and the events that trigger a change of state. Because the state changes are directly related to external trigger events from either IAS or IRIS, the diagram is annotated with a reference to IAS and IRIS’ interactions with CMS.

S 15, S 21

Figure 9: PAN States within CMS

3.2.2. MBUN States within CMS

CMS also manages the mapping of an MBUN to a PAN. The following diagram shows the set of states of an MBUN (representing an active or in-use card) and the events that trigger a change of state. As in the above diagram, the diagram is annotated with a reference to IAS interactions with CMS that explain the external trigger events.

S 15, S 21

Figure 10: MBUN States within CMS

3.2.3. MBUN States within IAS

IAS manages the mapping of an MBUN to a PAN. The following diagram shows the set of states of an MBUN (representing an active or in-use card) and the events that trigger a change of state. As in the above diagram, the diagram is annotated with a reference to IAS interactions with CMS that explain the external trigger events.

S 15, S 21

Figure 11: MBUN States within IAS

3.2.4. Credential Reference States within IAS

IAS also manages the mapping of an MBUN to an identity; this is abstractly labelled as a "credential reference". The IAS generates a credential reference when it registers an ICBC-issued card, then assigns it to the MBUN. The assignment of card (MBUN) to credential reference to identity is persistent over time, including after a card is expired or cancelled or an identity is marked as deceased or fraudulent.

4. TECHNICAL AND SECURITY DESIGN

This section of the document describes the detailed technical and security related design of the interfaces described in the previous section related to the BC Services Card program that are in scope for the issuance and management of cards.

4.1. SFTP Communications

IAS and CMS will exchange data using records in XML format and exchanged on a regular basis using the SFTP communications pattern. SecureKey will host an SFTP server where IAS will “put” files for CMS to “get”, and where CMS will “put” files for IAS to “get”.

The following diagram illustrates the pattern for IAS to send CMS card status update files, and for CMS to send confirmation files and operational reports.

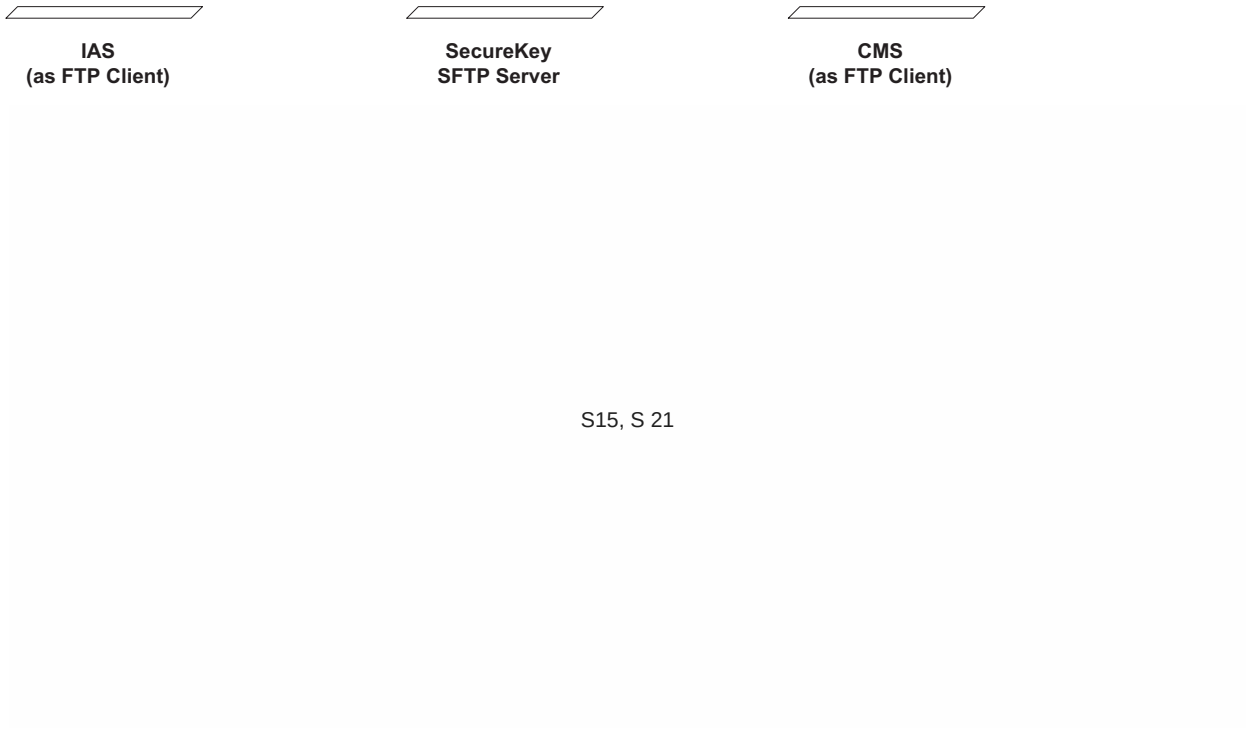


Figure 12: SFTP Pattern for File Exchange

SFTP communications will be authenticated using RSA Public/Private Key Pair; there will be an exchange of public keys to support this. For details of how Public keys will be exchanged please refer to section D.5.3 Key Ceremony Procedure.

4.2. File Processing

IAS and CMS will exchange data using records in XML format and exchanged on a regular basis. The following describes the file processing pattern in more detail.

Table 10: File Processing Steps

Processin_ Ste s
S15, S 21

Page 35 redacted for the following reason:
- -
S15, S 21

The following table lists the interfaces, as described in section 2, with file naming convention that includes a sequence number and date.

Table 11: File Naming Conventions

#	Interaction Type	File Type	Example
1.	Activate PANs		
2.	Deactivate PANs (aka “End of Life”)		
3.	Deactivate MBUNs (aka “End of Life”)		
4.	Suspend/Unsuspend MBUNs		
5.	Confirmation of Card Status Updates (Activate PANs)		
6.	Confirmation of Card Status Updates (Deactivate PANs)		
7.	Confirmation of Card Status Updates (Deactivate MBUNs)	S 15, S 21	
8.	Confirmation of Card Status Updates (Suspend/Unsuspend MBUNs)		
9.	Report of Card Status Updates		
10.	Report of Service Restores		
11.	Report of Operational Support		

Page 37 redacted for the following reason:
- -
S15, S 21

4.3. Technical Environments

IAS and CMS will each be deployed to several technical environments for development and testing purposes, before being deployed to an operational production environment. Further details will be provided in a separate document about testing and integration; the following is provided as a high level deployment view.

4.3.1. Integration Testing

LCTZ will deploy a test version of IAS to a test environment for the purpose integrated testing with SecureKey. SecureKey will also deploy a test version of CMS and SFTP server to a test environment. The test SecureKey SFTP server will be accessible over the internet by IAS during testing periods.

The test environment as described will remain after the initial project release to support ongoing testing and change management.

4.3.2. Production

LCTZ will deploy a production version of IAS to a production environment composed of multiple server nodes across two data centres (primary and failover). SecureKey will also deploy a production version of CMS and SFTP server to a production environment. The production SecureKey SFTP server will be accessible over the internet by IAS.

4.4. Security Requirements

As described in the above section, IAS and CMS will exchange data using the SFTP communications pattern. The following table lists the security requirements related to the file exchange.

Table 14: Security Requirements of File Exchanges

#	Security Requirement	Implication to IAS and CMS
1.	All PAN data shall be encrypted at rest.	PAN data will be encrypted by IBM as per Appendix A; IAS will receive the encrypted PAN data element as an opaque string such that IAS will not be able to know the PAN. CMS will decrypt the PAN data element and store in CMS using database encryption techniques. IAS would not need to encrypt any other data elements; encrypting the file contents is sufficient, as per the following security requirement.
2.	All data elements shall be encrypted at rest.	IAS will encrypt the contents of each XML file related to card status updates. Files on the SecureKey SFTP server will remain encrypted. XML encryption techniques will be used. Acceptable encryption algorithms: S 15, S 21 CMS does not need to encrypt the contents of each XML file related to confirmation and reports, as it is not specific and personal information; transport layer encryption is sufficient, as per the following security requirement.
3.	All data transmission shall be encrypted.	IAS and CMS will exchange files with the SecureKey SFTP server using SFTP protocol. This provides a secure tunnel for sending data files between two endpoints.

4.	The data transmission shall require mutually authenticated nodes.	IAS and CMS will each have public/private key pair for use with the SecureKey SFTP server. The SecureKey SFTP server itself will also have public/private key pair. Keys will be exchanged between each pair as per Appendix D – Security Design. Public/Private must be based on the RSA algorithm with a minimum key length of 2048 bits.
5.	Certificates/Keys shall be valid up to 2 years from issuance, and shall be replaced yearly.	This applies to each of the following certificates/keys, as per above security requirements: - IBM/CMS PAN encryption - IAS/SecureKey XML file encryption - IAS SFTP client authentication & transport encryption - CMS SFTP client authentication & transport encryption - SecureKey SFTP server authentication & transport encryption S 15
6.	All data shall be protected from unauthorized use.	IAS and CMS will each have internal access controls to prevent unauthorized access by staff within their organizations. The SecureKey SFTP server will have access controls to prevent unauthorized access to files, such that only IAS and CMS can “get”, “put” and “move” their appropriate set of files.

APPENDIX A – REQUIREMENTS FOR IBM AND ICBC

The purpose of this section is to describe the PAN data element security requirements specific to IBM card production that are relevant to IAS and CMS.

A.1 Requirements for PAN data

As described in section 2.1 “Activate PANs” and section 2.2 “Deactivate PANs”, the following PAN data element is required to be sent from IAS to CMS. The data element needs to be formulated by IBM in a format that SecureKey CMS can parse. IBM can obtain the PAN data by reading the card and/or cross-referencing the card stock mapping file from IRIS.

S 15, S 21

S 15, S 21 Before storing or sharing the PAN data element, it needs to be encrypted according to the following encryption approach. After it is encrypted, the PAN data element is considered a simple string of less than 256 characters that can be stored and passed between systems.

S15, S 21

S15, S 21

APPENDIX B – OPERATIONAL PROCEDURES

B.1 Initial List of Operational Procedures

The table below lists an initial set of operational procedures required by the LCTZ and SecureKey organizations to manage the ongoing production operations of the interfaces between IAS and CMS. This is not meant to be an exhaustive or well-described list. These operational procedures and others will be further described in a separate document focused on operational management between the two organizations.

Table 15: Initial List of Operational Procedures

#	Operational Procedure	Relevance to IAS and CMS
1.	Incident Management	- when a file is not available on the server at a specified time - when there are errors reading or decrypting a file - when a confirmation file indicates "FAILED"
2.	Resolve Discrepancies	- when a CMS-issued report file does not match the IAS data
3.	Key Management	- when renewed certificates need to be exchanged to authenticate endpoints, encrypt files, etc. - how keys are exchanged and kept secure
4.	Change Management	- when a software, hardware or configuration change is needed to remedy a defect, upgrade to keep current, etc. - when an interface change is needed to improve operations
5.	Problem Management	- when there are more incidents, discrepancies or service outages than expected

APPENDIX C – FILE STRUCTURES

C.1 Data Elements for File Header (for all files)

The data elements that are included any file are listed in the following table. The detailed schema is provided at the end of this Appendix.

Table 16: Data Elements for File Headers

#	Data Element Name	Description	Data Format & Rules	Cross reference to XML schema
1.	File Name	The name of the file.	Optional String, following the file naming convention of file type, sequence number and date, as listed in section 4.2.	
2.	File Schema Version	The version number of the schema that is used in this file.	Required String, default “v1.0”	
3.	File Timestamp	The date and time when the file was created by IAS in preparation for providing to CMS.	Required Date & Time	S 15
4.	File Author	The name of the organization that is providing the file.	Required String, default when file is created by IAS: “Province of BC”	
5.	File Record Count	The count of all records within the file.	Required Integer	
6.	Comments	A description to supplement the meaning of the file.	Optional String Should be provided to explain the purpose of the file if the file is not the original	

Pages 45 through 57 redacted for the following reasons:
- -
S15, S 21

APPENDIX D – SECURITY DESIGN

D.1 Network Level Security Controls

The network layer security will utilize SFTP as per SFTP Communications section of this document. SFTP will be configured to negotiate AES-256-CBC for encryption.

D.2 File Level Security Controls

D.2.1 File Transfer from IAS to SecureKey

X.509 Certificates will be used to support XML Encryption/Signing. Both LCTZ and SecureKey will procure X.509 Certificates on yearly basis. LCTZ will get its certificates from PWGSC CA. SecureKey will get its certificates from external certificate authority such as Entrust or Verisign.

The diagram below summarizes the proposed flow for performing XML Encryption/Signing for files sent from IAS to SecureKey

S15, S 21

For samples of XML signed and encrypted files please see Appendix E – Sample Signed File and Appendix F – Sample Encrypted File respectively.

D.2.2 File Transfer from SecureKey to IAS

SecureKey does not need to encrypt the contents of each XML file related to confirmation and reports, as it is not specific and personal information; transport layer encryption is sufficient, as per security requirement #2 in Security Requirements section.

D.3 Field Level Security Controls

PAN data will be encrypted by IBM; IAS will receive the encrypted PAN data element as an opaque string such that IAS will not be able to know the PAN. S 15

S 15

D.4 Certificate/Key Summary

The table below summarises all of the keys involved in the Security Design. The keys are broken into four categories:

- IAS Internal Keys: Keys are generated at IAS and are never shared with CMS
- CMS Internal Keys: Keys are generated at CMS and are never shared with IAS
- IAS-CMS Session Keys: Keys are negotiated by SFTP and XML protocols automatically
- IAS-CMS Shared Keys: Keys are shared between CMS and IAS as per defined key ceremony

Table 17: Certificate/Key Summary

S15, S 21

o es:

1. Generation and exchange of this key is governed by SFTP protocol.

D.5 Key Ceremony Procedure

The following is a conceptual overview of the Key Ceremonies used by LCTZ and SecureKey to exchange all of the keys. For details of these procedures please refer to the appropriate operational documents.

D.5.1 Key Ceremonies Checklist

S15, S 21

D.5.2 One Time Exchange

This procedure describes a onetime key ceremony for exchanging Government of Canada root certificate. (This procedure must be repeated if LCTZ will switch to British Columbia CA in a future)

S15, S 21

Page 62 redacted for the following reason:
- -
S15, S 21

Table 18: OpenSSL commands to support key exchange

S15, S 21

D.6 Key Compromise Procedure

In case Key Compromise is detected all of the key ceremonies described in D.5.3 Key Ceremony Procedure must be redone. For more details regarding operationalization of Key Compromise Procedures please refer to the appropriate documents.

APPENDIX E – SAMPLE SIGNED FILE

S15, S 21

APPENDIX F – SAMPLE ENCRYPTED FILE

S15, S 21

CMS PROGRAM WIDE SECURITY DESIGN

Document Control Change Record

Date	Revision	Section(s)	Editor	Change Reference
05/08/2012	0.1		Eli Erlikhman	Initial draft template
05/15/2012	0.2		Eli Erlikhman	Updated to include latest design changes
05/18/2012	0.3		Eli Erlikhman	Updated based on design discussions with BC
05/22/2012	0.4		Eli Erlikhman	Updated based on design discussions with Bell ID and integrated material from latest Key Exchange document from Bell ID
05/25/2012	0.5		Eli Erlikhman	Updated based on review with Bell ID
05/30/2012	1.0		Eli Erlikhman	Made final changes based on discussions with Bell ID, CITX and IRIS.
06/6/2012	1.1	All	Eli Erlikhman	Restructured document and started working on section 3
06/13/2012	1.2	3	Eli Erlikhman	Completed section 3 of the document for IRIS
06/21/2012	1.3	4-11	Eli Erlikhman	Finished IRIS assessment findings
06/21/2012	1.4	All	Dmitry Barinov	Final edits
07/18/2012	1.5	All	Eli Erlikhman	Updated document based on feedback from BC
08/01/2012	1.6	All	Eli Erlikhman	Added details on SecureKey and IBM based on IBM design document
09/12/2012	1.7		Eli Erlikhman	Updated based on feedback from BC
09/27/2012	1.8		Dmitry Barinov	Updated based on IBM assessment
10/29/2012	1.9		Eli Erlikhman	Updated based on BC feedback
11/09/2012	2.0		Chris Chapman	Updated BC SK Approvals

Document Approvers

Name, Title	Approved by Email	Date
Dmitry Barinov Chief Architect, CSO SecureKey Technologies, Inc.	Approved	November 9 2012
Ian Bailey ED Architecture & Standards and A/CISO, Office of the CIO CITZ, Province of BC	Approved	November 9 2012

Document Reviewers

Representing Province of BC	Representing SecureKey
Henry Lee Senior Manager, Information Security Program, Office of the CIO CITZ	Eli Erlikhman Director Security Architecture SecureKey Technologies, Inc
Patricia Wiebe Director and Solution Architect Office of the CIO CITZ, Province of BC	Ayinde Yakubu Solution Architect SecureKey Technologies, Inc
	Chris Chapman Project Delivery Manager SecureKey Technologies, Inc

Table of Contents

Figures

Tables

Referenced Documents

[IAS_INT_DESIGN]	IAS and CMS Interface Design Specifications
[IBM_PAN_DESIGN]	IBM Card Production PAN Data Management Design
[IRIS_ARCH]	IRIS Security Architecture of System and Network
[IRIS_AUDIT]	IRIS Letter of Compliance Audit for ISO 27001:2005
[IRIS_INT_DESIGN]	IRIS and SecureKey Interface Design Specifications
[IRIS_ISMS]	IRIS Information Security Management System Manual
[IRIS_KEY]	IRIS Key Management System Procedure
[IRIS_PCI]	IRIS PCI Attestation Report
[IRIS_VISA]	IRIS Visa Inspection Certificate
[SK_SEC_REQ]	Security Requirements for BC Services Card Program: SK-RE010
[SK-KM0002]	SecureKey Key Custodians Master List
[SK-KM0010]	SecureKey Key Database
[SK-KM0101]	SecureKey CMS Internal KEK_VSDC Key Generation Ceremony
[SK-KM0102]	SecureKey CMS Internal KEK_PAN Key Generation Ceremony
[SK-KM0401]	SecureKey ZMK Export Key Ceremony
[SK-KM0402]	SecureKey ZMK Import Key Ceremony
[SK-KM0403]	SecureKey ENC_IRIS and HMAC_IRIS Export Key Ceremony
[SK-KM0406]	SecureKey TK_IRIS Generation & Export Key Ceremony
[SK-KM0407]	SecureKey IMK_AC First Key Generation & Export Key Ceremony
[SK-KM0408]	SecureKey CMS_IBM RSA Key Pair Generation & Export Key Ceremony
[SK-KM0409]	SecureKey TK_IBM Import Key Ceremony
[SK-KM0410]	SecureKey CMS_XML Certificate Generation & Export Key Ceremony
[SK-KM0411]	SecureKey IAS_XML Certificate Import Ceremony
[SK-KM0601]	SecureKey ZMK_IRIS Key Ceremony
[SK-KM0602]	SecureKey SFTP_IRIS Key Ceremony

[SK-KM0604]	SecureKey ENC_IRIS HMAC_IRIS Key Ceremony
[SK-KM0605]	SecureKey TK_IRIS Key Ceremony
[SK-KM0606]	SecureKey IAS SK Key Ceremony
[SK-KM0607]	SecureKey IAS IBM Key Ceremony
[SK-MA001]	SecureKey Security Manual
[SK-MA005]	SecureKey IT Procedures Manual
[SK-PC001]	SecureKey Information Security Policy
[SK-PC002]	SecureKey Asset Management Policy
[SK-PC003]	SecureKey Human Resources Security Policy
[SK-PC004]	SecureKey Physical and Environmental Security Policy
[SK-PC005]	SecureKey Access Control Policy
[SK-PC006]	SecureKey Security Incident Management Policy
[SK-PC007]	SecureKey Information Systems Acquisition, Development and Maintenance Policy
[SK-PC008]	SecureKey Communications and Operations Management Policy
[SK-PC009]	SecureKey Business Continuity Management Policy
[SK-PC010]	SecureKey Compliance Policy
[SK-PC011]	SecureKey Privacy Policy
[SK-PR005]	SecureKey Security Vulnerability and Patch Alerting Procedure
[SK-PR006]	SecureKey Change Management Procedure
[SK-SEC_DEV]	SecureKey Security Testing Framework
[SK-ST001]	SecureKey Encryption Standard
[SK-TRANSITION]	BC Services Card Transition Design Specification
[VISA_KEY]	VISA KeyRequests_SecureKey_2012_JUN_11.pdf

1. Introduction

1.1 Purpose

The purpose of this document is to define the overall Security Design and Security Controls for the Card Management System (CMS). Security Design and Security Controls is documented for the following parties:

1. SecureKey
2. IRIS
3. IBM
4. CITZ
5. ICBC

1.2 In Scope

The following items are in scope of this document:

- Security Requirements for the following parties:
  - SecureKey
  - IRIS

    - IBM
    - CITZ
    - ICBC
- Implemented Security Controls for the following parties:
    - SecureKey
    - IRIS
    - IBM
    - CITZ
    - ICBC
- Security Design of CMS System managed by SecureKey
- Overview of Security Design by IRIS in order to support production of BC Service Card
- Overview of Security Design by IBM in order to support production of BC Service Card
- Overview or procedural controls for:
    - SecureKey
    - IRIS
    - IBM

1.3 Out of Scope

The following items are explicitly out of scope of this document:

- Security Design of systems impacted at CITZ and ICBC

Security Design of communication channels between IBM and BC Systems

2. Security Requirements & Controls

Security Requirements and Controls are categorized into the following functional areas:

1. Card Inventory Management during Manufacturing & Production
2. Card Delivery and Returned Mail Handling
3. Card Data Exchange and Data Management
4. Secret Key Exchange and Key Management
5. Network and Systems Environment
6. Vulnerability Management
7. Access Control Measures
8. Monitoring and Testing
9. Information Security Policy

For more details on these requirements please refer to [SK_SEC_REQ]. The table below provides a high level summary of these requirements and how they apply to various stakeholders:

Category	Req #	Requirement	Secure Key	IRIS	IBM	CITZ	ICBC
Card Inventory Management			S 15, S 21				

Category	Req #	Requirement	Secure Key	IRIS	IBM	CITZ	ICBC
Card Delivery and Returned Mail Handling			S 15, S 21				
Card Data Exchange and Data Management							

Category	Req #	Requirement	Secure Key	IRIS	IBM	CITZ	ICBC
			S 15, S 21				

Category	Req #	Requirement	Secure Key	IRIS	IBM	CITZ	ICBC
Secret Key Exchange and Key Management			S 15, S 21				
Network and Systems Environment							

Category	Req #	Requirement	Secure	IRIS	IBM	CITZ	ICBC
			S 15, S 21				
Vulnerability Management							
Access Control Measures							

Category	Req #	Requirement	Secure	IRIS	IBM	CITZ	ICBC
Monitoring and Testing			S 15, S 21				
Information Security Policy							

Category	Req #	Requirement	Secure	IRIS	IBM	CITZ	ICBC

S 15, S 21

3. Card Inventory Management during Manufacturing and Production

This section of the Security Design applies to IRIS and IBM only. Summary of the Security Assessment performed by SecureKey at IRIS and IBM is summarized.

3.1 Card Inventory Management Controls at IRIS

IRIS has developed both procedural and technical/physical controls in order to meet the necessary security controls for Card Inventory Management during manufacturing. These controls are in place for BC Card manufacturing as well as for other payment card manufacturing processes undertaken by IRIS. These controls are designed based on the VISA standards and are subject to annual verification by VISA.

3.1.1 Procedural Controls Overview

Procedure Category	Procedure Description	Assessment Summary
Card Inventory Management		S 15, S 21

Procedure Category	Procedure Description	Assessment Summary
Missing Card Inventory Management		S 15, S 21

Procedure Category	Procedure Description	Assessment Summary
Card Shipping		S 15, S 21

Procedure Category	Procedure Description	Assessment Summary
Regular Card Status Updates		
Information System Documentation		S 15, S 21

3.1.2 Technical and Physical Controls Overview

Controls in scope for Card Inventory Management are:

- Physical controls for access to secure room containing card inventory
- Technical access controls for access to secure room containing card inventory

IRIS has the following technical and physical controls in place for secure room used for storing cards:

- IRIS facility is a secure facility with 724 monitoring and security guards on site

- Secure Room is located within internal security perimeter
- Secure room is only accessible to authorized personnel
- Access to the secure room is provisioned through a central system by access administrator
- Access List to the secure room is separate from access to the building and to the internal security perimeter
- Entrance to the secure room is monitored 24x7
- Secure room has fire detection in place

3.2 Card Inventory Management Controls at IBM

The description of Card Inventory Management Controls at IBM is based on the information provided in [IBM_PAN_DESIGN] document and site visit to IBM facilities performed by SecureKey.

3.2.1 Procedural Controls Overview

Procedure Category	Procedure Description	Assessment Summary
Card Inventory Management		S 15, S 21
Missing Card Inventory Management		

Procedure Category	Procedure Description	Assessment Summary
Secure Card Storage		
Regular Card Status Updates		S 15, S 21
Information System Documentation		

3.2.2 Technical and Physical Controls Overview

Controls in scope for Card Inventory Management are:

- Physical controls for access to secure room containing card inventory
- Technical access controls for access to secure room containing card inventory

IBM /BCMP has the following technical and physical controls in place for secure room used for storing cards:

- IBM/BCMP facility is a secure facility with 24x7 monitoring and security guards on site during the day time
- Facility is not operated during night (no 3rd shift)
- Secure Room is located within internal security perimeter
- Secure room is only accessible to authorized personnel
- Access to the secure room is provisioned through a central system by access administrator
- Access List to the secure room is separate from access to the building and to the internal security perimeter
- Entrance to the secure room is monitored 24x7
- Secure room has fire detection in place

4. Card Delivery and Returned Mail Handling

4.1 Card Delivery at IBM

The description of Card Delivery Controls at IBM is based on the information provided in [IBM_PAN_DESIGN] document and site visit to IBM facilities performed by SecureKey.

4.1.1 Procedural Controls Overview

Procedure Category	Procedure Description	Assessment Summary
Mailing of cards to the cardholder in secure manner		S 15, S 21
Secure Room Processes		

Procedure Category	Procedure Description	Assessment Summary
Procedures for tracking and providing card status updates to SecureKey		S 15, S 21

4.2 Card Delivery and Returned Mail Handling at CITZ and ICBC

The following Card Delivery and Returned Mail requirements from [SK_SEC_REQ] are applicable to CITZ and ICBC:

#	Requirement
CD-005	Keep track of when and where cards were mailed from and to
CD-006	Provide weekly card status updates about mailed cards to SecureKey electronically in a secure manner
CD-007	Provide weekly card status updates about spoiled cards to SecureKey electronically in a secure manner
CD-008	Keep track of when cards are returned undelivered and when cards are resent to cardholders.
CD-009	Provide card status updates about returned and resent mail to SecureKey electronically in a secure manner when requested for card inventory accounting purposes, approximately semi-annually.

Documentation of how these requirements are addressed by CITZ and ICBC are outside the scope of this document.

5. Card Data Exchange and Data Management

5.1 Card Data Exchange and Data Management at IRIS

IRIS has developed both procedural and technical controls in order to meet the necessary security controls for Card Data Exchange and Data Management.

5.1.1 Procedural Controls Overview

Procedure Category	Procedure Description	Assessment Summary
Protection of card holder data		S 15, S 21

Procedure Category	Procedure Description	Assessment Summary
Access to card holder data		
Network and Communication Controls		S 15, S 21
Government standard cryptographic controls		
Other Controls		

Procedure Category	Procedure Description	Assessment Summary
		S 15, S 21

5.1.2 Technical Controls Overview

5.1.2.1 Network Security Architecture

S 15, S 21

5.1.2.2 Security Testing

IRIS has undergone Security Penetration testing of its external facing Internet applications. Penetration Testing was done in accordance with PCI DSS requirements. Penetration Testing was done by an ASV (Approved Scanning Vendor) as mandated by PCI DSS.

The latest Penetration Testing report was produced on April 18th, 2012. No vulnerabilities were identified.

Penetration Testing by ASV is done on quarterly basis as mandated by PCI DSS.

5.1.2.3 VISA Certification

IRIS undergoes VISA Certifications on yearly basis. The latest VISA certification was produced by VISA on January 1st 2012 and it is valid for the remainder of the calendar year.

VISA Certification confirms that IRIS

"have been assessed by VISA and found to have met the applicable security requirements and guidelines to Visa's satisfaction with regard to the scope of this certificate:

- Magnetic Stripe Personalizer
- IC Personalizer"

5.1.2.4 Data Protection

S 15, S 21

IRIS encrypts files (XML files) to SecureKey within Secure Room. Encrypted files are physically moved to Server within IRIS internal network. Files are pushed from the Server to SFTP Server.

5.1.2.5 Access Controls

IRIS has implemented strong access controls to its Secure Room. These access controls include:

- Auditable log of people accessing Secure Room
- Auditable log of equipment/data moved to the Secure Room. This includes
  - Blank cards
  - Personalized Cards
  - Encrypted files exchanged with 3rd parties
- Access rights are only granted to authorized personnel
- 24x7 video surveillance

5.2 Card Data Exchange and Data Management at IBM

The description of Card Data Exchange and Data Management at IBM is based on the information provided in [IBM_PAN_DESIGN] document and site visit to IBM facilities performed by SecureKey.

5.2.1 Procedural Controls Overview

Procedure Category	Procedure Description	Assessment Summary
Protection of card holder data		S15, S 21
Access to card holder data		

Procedure Category	Procedure Description	Assessment Summary
Network and Communication Controls		S 15, S 21
Government standard cryptographic controls		
Other Controls		

5.2.2 Technical Controls Overview

Please refer to Appendix C: IBM Solution Overview of this document for diagrams providing an overview of:

1. Flow of data, cards, etc within IBM systems
2. Flow of PAN within IBM systems

In summary:

1. IBM has dedicated facilities for Secure card storage
2. IBM has dedicated facilities for Laser Engraving
3. IBM has dedicated facilities for Inventory Control
4.
5.

S15, S 21

6.
7.

5.3 Card Data Exchange and Data Management at SecureKey

5.3.1 Procedural Controls Overview

Procedure Category	Procedure Description	Assessment Summary
Protection of card holder data	Protection of card holder data in transmission	SecureKey has a number of policy documents that describe the appropriate security controls for protecting confidential data. Card holder data is classified as confidential. Some of the applicable policy documents are: • [SK-PC001] • [SK-PC005] • [SK-PC010] SecureKey also implemented strong security controls to protect card holder data in transmission. Sensitive cardholder data such as PAN is always encrypted in transmission. S 15, S 21
	Protection of card holder data in storage	

Procedure Category	Procedure Description	Assessment Summary
Access to card holder data	Access Authentication	
	Access Logging	S 15, S 21
Network and Communication Controls	Security Network Controls	

Procedure Category	Procedure Description	Assessment Summary
	Data Sharing with External Parties	
	Use of Secure Communication Protocols	
Government standard cryptographic controls	Encryption algorithms and controls	
	Authentication algorithms and controls	
Other Controls	Security Testing	S 15, S 21

Procedure Category	Procedure Description	Assessment Summary
	System updates	S 15, S 21
	System operations	

5.3.2 Technical Controls Overview

The details of technical controls are documented in SecureKey Security Design section of this document.

6. Secret Key Exchange and Key Management

6.1 Secret Key Exchange and Key Management at IRIS

IRIS has developed both procedural and technical controls in order to meet the necessary security controls for Secret Key Exchange and Key Management.

6.1.1 Procedural Controls Overview

Procedure Category	Procedure Description	Assessment Summary
Key Management Configuration	Hardware Configuration	S15, S 21
	Production vs Test environment	
	Key Management roles	
	Software Setup	

Procedure Category	Procedure Description	Assessment Summary
	HSM Management	
Roles & Responsibilities	Documented Roles & Responsibilities	
	Appointment letters	S 15, S 21
	Termination & Replacement	
Key Management Activities	Procedures for key exchange	

Procedure Category	Procedure Description	Assessment Summary
	Password Management	
	Key Management	
		S 15, S 21
	Safe Management	
	Training	

6.1.2 Technical Controls Overview

The following documents were reviewed at IRIS to evaluate technical controls:

- [IRIS_ARCH]
- [IRIS_AUDIT]
- [IRIS_ISMS]
- [IRIS_KEY]
- [IRIS_PCI]

- [IRIS_VISA]

IRIS has the following stations for Key Management and Data preparation

1. Key Management Station
    a. Responsible for managing all of the keys
    b. Not connected to any network. Completely offline
2. Data Preparation Station
    a. Responsible for doing data preparation
    b. Not connected to any network. Completely offline
3. Production Station
    a. Responsible for card personalization

IRIS has dedicated safes for storing the following information:

S 15, S 21

There are separate safes for different roles with KMS. These safes are:

S 15, S 21

6.2 Secret Key Exchange and Key Management at IBM

The description of Secret Key Exchange at IBM is based on the information provided in [IBM_PAN_DESIGN] document and site visit to IBM facilities performed by SecureKey.

6.2.1 Procedural Controls Overview

These are described in [IBM_PAN_DESIGN] document in attachment.

Procedure Category	Procedure Description	Assessment Summary
Key Management Configuration	S 15, S 21	

Procedure Category	Procedure Description	Assessment Summary
Roles & Responsibilities		
Key Management Activities		S 15, S 21

6.2.2 Technical Controls Overview

IBM has documented technical controls around Key Exchange with IRIS and SecureKey in [IBM_PAN_DESIGN] document in Appendix B: Interface Design Specifications.

S 15, S 21

IBM exchanges keys with SecureKey on annual basis using procedures and controls documented in [IBM_PAN_DESIGN] document in Appendix B: Interface Design Specifications and SK-KM0607.

6.3 Secret Key Exchange and Key Management at SecureKey

6.3.1 Procedural Controls Overview

Procedure Category	Procedure Description	Assessment Summary
Key Management Configuration		S15, S 21

Procedure Category	Procedure Description	Assessment Summary
Roles & Responsibilities		
Key Management Activities		S 15, S 21

Procedure Category	Procedure Description	Assessment Summary
		S 15, S 21

6.3.2 Technical Controls Overview

Please refer to SecureKey Security Design section of this document

6.4 Secret Key Exchange and Key Management at CITZ

The following Secret Key Exchange and Key Management requirements from [SK_SEC_REQ] are applicable to CITZ:

#	Requirement
KM-001	Exchange keys and certificates using a secure channel
KM-002	Exchange keys and certificates in a manner that is auditable
KM-003	Exchange keys and certificates in a manner that verifies the identity of the sender out-of-band from the exchange
KM-004	Establish keys and certificates for specific and defined purposes, and use them only for those purposes (e.g., encryption keys are not used for signing.)
KM-005	Store keys and certificates in a secure manner
KM-006	Log system and user access to keys and certificates
KM-007	Renew the usage, strengths and validity of keys and certificates on an annual basis

The following table provides a reference of where these requirements are documented in project documents.

[IAS_INT_DESIGN]

SK_SEC_REQ] Requirement	Reference Documentation
KM-001	Details of the exchange of the applicable keys and certificates are documented in [SK-KM0606] High level summary of these procedures are documented in section D.5 of [IAS_INT_DESIGN]
KM-002	Details of the exchange of the applicable keys and certificates are documented in [SK-KM0606] High level summary of these procedures are documented in section D.5 of [IAS_INT_DESIGN]
KM-003	Details of the exchange of the applicable keys and certificates are documented in [SK-KM0606] High level summary of these procedures are documented in section D.5 of [IAS_INT_DESIGN]

KM-004	The requirements for all keys is documented in section 4.4 of [IAS_INT_DESIGN] All Keys are documented in section D.4 of [IAS_INT_DESIGN]
KM-005	This requirement would need to be addressed by CITZ internal documentation
KM-006	This requirement would need to be addressed by CITZ internal documentation
KM-007	Requirement #5 in section 4.4 of [IAS_INT_DESIGN]

7. Network and Systems Environment

7.1 Network and Systems Environment at IRIS

Procedure Category	Procedure Description	Assessment Summary
Network Environment and Architecture		
Management of Network Configuration		S 15, S 21
Personal		

Procedure Category	Procedure Description	Assessment Summary
Devices	S 15, S 21	
Installation and Configuration of Card Holder Data Management System		

7.2 Network and Systems Environment at IBM

The description Network and Systems Environment at IBM is based on the information provided in [IBM_PAN_DESIGN] document and site visit to IBM facilities performed by SecureKey.

Procedure Category	Procedure Description	Assessment Summary
Network Environment and Architecture	S 15, S 21	
Management of Network Configuration		

Procedure Category	Procedure Description	Assessment Summary
Personal Devices		
Installation and Configuration of Card Holder Data Management System		S 15, S 21

7.3 Network and Systems Environment at SecureKey

Procedure Category	Procedure Description	Assessment Summary
Network Environment and Architecture		
Management of Network Configuration		S 15, S 21

Procedure Category	Procedure Description	Assessment Summary
Personnel Devices		S 15, S 21
Installation and Configuration of Card Holder Data Management System		

8. Vulnerability Management

8.1 Vulnerability Management at IRIS

S 15, S 21

8.2 Vulnerability Management at IBM

Vulnerability management of network devices is performed by IBM MSS service.

S 15, S 21

Engraving machines are updated from S 15, S 21 on a regular basis.

8.3 Vulnerability Management at SecureKey

Vulnerability management policy is documented in [SK-PC007].

Vulnerability management procedures are documented in in [SK-PR006]

Vulnerability management during software development lifecycle are documented in [SK-SEC_DEV]

9. Access Control Measures

9.1 Access Control Measures at IRIS

The details of this assessment are documented in various parts of sections 3 through 8. In summary:

- IRIS has documented procedures to grant access to systems based on need-to-know basis and split knowledge where needed

9.2 Access Control Measures at IBM

IBM personnel onsite has S 15, S 21 in steady state.

Access controls is managed through Consolidated Resource registry. This document lists access rights of IBM employees at facilities.

Separation of Duties document covers all roles and all tasks of the employees on the project.

9.3 Access Control Measures at SecureKey

The details of this assessment are documented in various parts of sections 3 through 8.

10. Monitoring and Testing

10.1 Monitoring and Testing at IRIS

Procedure Category	Procedure Description	Assessment Summary
Logging & Monitoring		
Testing	S 15, S 21	

10.2 Monitoring and Testing at IBM

The description of Monitoring and Testing at IBM is based on the information provided in [IBM_PAN_DESIGN] document and site visit to IBM facilities performed by SecureKey.

Procedure Category	Procedure Description	Assessment Summary
Logging &	S 15, S 21	

Procedure Category	Procedure Description	Assessment Summary
Monitoring		
Testing		S 15, S 21

10.3 Monitoring and Testing at SecureKey

Procedure Category	Procedure Description	Assessment Summary
Logging & Monitoring		
Testing		S 15, S 21

11. Information Security Policy

11.1 Information Security Policy at IRIS

Procedure Category	Procedure Description	Assessment Summary
Information Security Policy		S 15, S 21
Incident Management		
PCI/VISA Compliance		

11.2 Information Security Policy at IBM

The description Information Security Policy at IBM is based on the information provided in [IBM_PAN_DESIGN] document and site visit to IBM facilities performed by SecureKey.

Procedure Category	Procedure Description	Assessment Summary
Information Security Policy		S 15, S 21
Incident Management		
PCI/VISA Compliance		

11.3 Information Security Policy at SecureKey

Procedure Category	Procedure Description	Assessment Summary
Information Security Policy	Information Security Policy	SecureKey has developed the following Information Security Policies: • [SK-PC001] • [SK-PC002] • [SK-PC003] • [SK-PC004] • [SK-PC005] • [SK-PC006] • [SK-PC007]

Procedure Category	Procedure Description	Assessment Summary
		• [SK-PC008] • [SK-PC009] • [SK-PC010] • [SK-PC011]
	Information Security Policy Review	SecureKey performs review of its Security policies on annual bases
	Review of IS Policy	S 15, S 21
	IS Responsibilities	
	Hiring Policy	
Incident Management	S 15, S 21	
PCI/VISA Compliance		

Procedure Category	Procedure Description	Assessment Summary
		S 15, S 21

12. SecureKey Security Design

12.1 Security Design Overview

EMV Key Manager is used to setup and manage the key material of the SecureKey BC solution. EMV Key Manager supports the key ceremony procedures to exchange key material between CMS and other systems

The following diagram shows all of the data flows between the various parties as known to SecureKey. Details of the data flows between IBM, ICBC and IAS are outside the scope of this document. For more details on data flows outlined in the diagram please refer to Data Flows Description section of this document.

S15, S 21

Figure 1: Data Flow Summary

The following diagram shows all of the key exchanges between the various parties. Keys displayed within SecureKey CMS box are not shared between CMS and any other parties. For more details on key exchanges outlined in the diagram please refer Key Exchange Description section of this document.

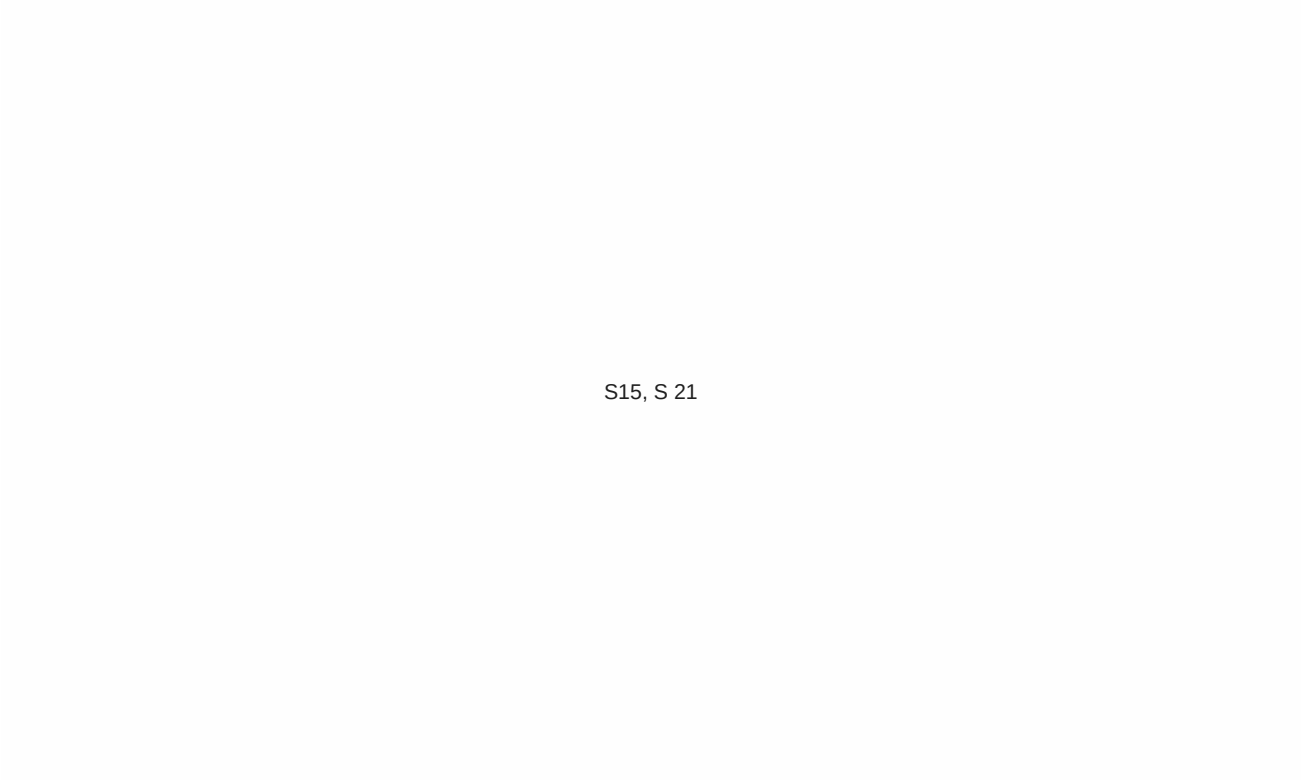


Figure 2: Key Flow Summary

Notes:

1. S 15
2. Keys exchanged between IBM, ICBC and IAS are not known to SecureKey and are outside the scope of this document.

12.2 Data Flows Description

The table below identifies all of the data flows and appropriate security controls for files and fields identified in a diagram presented in Security Design Overview.

Table 1: Data Flows Description

S15, S 21

12.3 Key Exchange Description

The table below identifies all of the key locations and exchange methods for keys identified in a diagram presented in Security Design Overview. The following keys are not displayed within this table:

1. Keys that are external to CMS and that are not shared with CMS
2. Session Keys generated as part of SFTP and XML Encryption protocols

Table 2: Ke Summar

S15, S 21	

S15, S 21

S15, S 21

12.4 P3 File Layout

The layout of P3 file is as depicted in the diagram below. For more details on P3 file layout please refer to sections 2.1 and 2.2 of SK_IRIS_Interface_Design_Specifications.

Table 4: P3 Record La out

S15, S 21

12.5 Network Level Security

S 15, S 21

12.6 Other Design Considerations

This section documents all other design considerations that are not explicitly stated in Section 2 of this document.

S15, S 21

S15, S 21

S15, S 21

12.8 Block Encryption and HMAC

S15, S 21

S15, S 21

12.9 XML Encryption and Signature

The following two flow charts show the processing steps for encrypting/signing XML files by the sender and verifying/decrypting block files by the receiver.

S15, S 21

12.10 Transition File Backup and Recovery Process

SecureKey has established a process for the backup and recovery of information for all BC Services cards stored within CMS system. The details of this process and described in [SK-TRANSITION] document. The following is the summary of the security controls around Transition File Backup and Recovery Process:

S15, S 21

Appendix A: Glossary

Term	Description
AC	Application Cryptogram used to authorize the card
CMS	Card Management System
DKI	Derivation Key Index
EPAN	Encrypted PAN
IAS	Identity Assurance Services
IBM	Organization that performs the plastic personalization of the service card
IRIS	Organization that performs the chip personalization of the service card
ISMS	Information Security Management System
MDK	Master Derivation Key
PAN	Primary Account Number
PayWave	Same as qVSDC
qVSDC	Quick VSDC, contactless EMV payment application from Visa
TM	EMV Token Manager, the Bell ID product solution to implement the SecureKey CMS

Appendix B: Interface Design Specifications

BCSC IAS CMS Interface Design Specifi

SK IRIS Interface Design Specification

BCSC IBM Card Production PAN Data

Appendix C: IBM Solution Overview

S15, S 21

S15, S 21

BC Services Card Project

LCTZ Partner Integration Testing Strategy

DRAFT

Version: 0.5
May 29, 2012

Document Information

This is a point-in-time version of a document. Please contact the author or the person who issued this document (listed below) if you are in any doubt about the currency of this document.

Document title	LCTZ Partner Integration Testing Strategy
Document file name	BCSC LCTZ Partner Integration Testing Strategy v0 5.docx
Revision number	0.5
Issued by	Patricia Wiebe (patricia.wiebe@gov.bc.ca)
Issue Date	May 29, 2012
Status	Draft

Document Purpose and Intended Audience

This document describes the testing strategy from Ministry of Labour, Citizens' Services and Open Government (LCTZ)'s perspective relevant to the initial release of the BC Services Card program. This document is intended to be an extension to the ICBC test strategy and the joint end to end system integration test strategy between ICBC and HIBC.

The scope of this document is focused on the testing strategy related to the functions and information exchanges for preparing cards with active chips, integrating ICBC and IAS systems, integrating IAS and SecureKey systems, and integrating IAS and Ministry of Health Client Registry systems.

This document is intended to facilitate alignment of effort and scope of the testing effort leading up to implementing the system into production in November, 2012. This document will also be used as the framework for detailed test planning.

Document References

The following documents are related to this document.

1. BCSC ICBC Test Strategy
2. BCSC ICBC-HIBC Joint End to End Test Strategy
3. BCSC ICBC and IAS Interface Design Specification
4. BCSC IAS and CMS Interface Design Specification
5. BCSC IAS and HCIM Interface Design Specification
6. BCSC Card Design Specification
7. BCSC Chip Profile Specification

Document Approvals

Name, Title	Signature	Date
Ian Bailey ED Architecture & Standards and A/CISO, Office of the CIO, LCTZ, Province of BC		
Kevena Bamford ED IDIM Service Delivery Shared Services BC, LCTZ, Province of BC		
Kathy Thomson Director of Driver Licensing Insurance Corporation of BC		
Andre Boysen EVP Digital Identity and Authentication SecureKey Technologies, Inc.		
Jack Shewchuk CEO Vital Statistics Agency Ministry of Health		

Document Reviewers

Representing LCTZ	Representing ICBC	Representing SecureKey	Representing Ministry of Health
Patricia Wiebe Director & Solution Architect Office of the CIO	Sam Van der Merwe Project Lead ICBC	Chris Chapman Project Delivery Manager SecureKey Technologies	Anita Malovec Manager, Health Registries Ministry of Health
Jeremy Moss Director, IDIM Business Development	Keith Rodrigue Business Analyst ICBC	Maggie Au Professional Services SecureKey Technologies	Kepmen Lee Business Analyst and Project Manager CGI, Inc
Jason Owens Test Lead IDIM Operations	Jody Webber Test Lead ICBC	TBD	TBD

Document Version History

Version	Revision Date	Author	Summary of Changes	Changes Marked?
0.1	Apr 16, 2012	Dana Kawas	Initial creation of outline	No
0.2	May 7, 2012	Patricia Wiebe Dana Kawas	Continued drafting of content	No
0.3	May 9, 2012	Patricia Wiebe Dana Kawas	Updated the document per Jeremy's Moss comments	Yes
0.4	May 11, 2012	Patricia Wiebe	Minor updates, ready for internal review	No
0.5	May 29, 2012	Patricia Wiebe	Minor updates, changed approach to allow for open discussion	No

Document Contents

Figures

Tables

1. TESTING OBJECTIVES

This test strategy is focused on the functional testing of partner system integrations for the initial release of the BC Services Card program in November, 2012. The scope of this document is the functions and information exchanges for preparing cards with active chips, and integrating ICBC, SecureKey and Ministry of Health systems with the Identity Assurance Services. The following list describes the objectives of this testing:

- Ensure all technical integrated system components function as designed;
- Ensure that data is processed according to the business rules in all systems; and,
- Ensure that an end to end test is performed on the systems that support the issuance of a BC Services Card.

2. TESTING SCOPE

The scope of this document is focused on the testing strategies related to preparing cards with active chips, and integrating LCTZ's IAS system with ICBC, SecureKey and Ministry of Health systems. This document is intended to supplement the testing strategies already under discussion between ICBC and HIBC.

The following diagram illustrates the high level solution architecture related to the processes of manufacturing cards and issuing cards to clients (BC residents). The diagram is a simplified view of the many information exchanges between the partner organizations involved in the BC Services Card program. The most notable simplification is that there are actually several additional information exchanges between ICBC and HIBC systems; refer to Health-ICBC-HIBC project documentation for more detail on the specific interfaces.

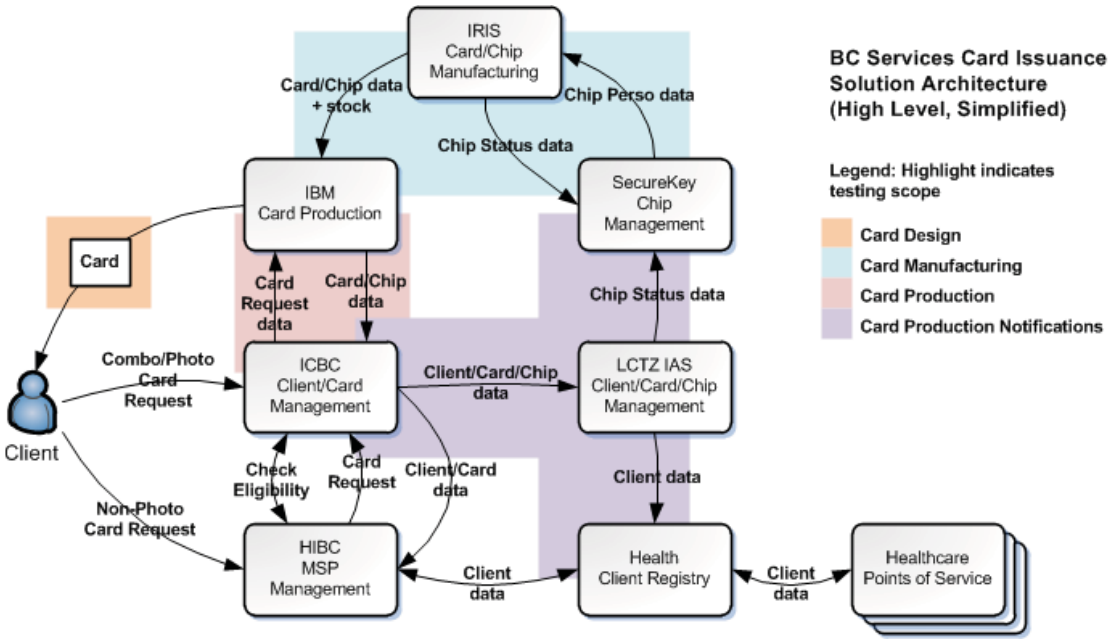


Figure 1 – High Level Solution Architecture with Highlighted Test Scopes

This diagram is provided to illustrate many information exchanges that are not shown in Health-ICBC-HIBC project documentation because it was not deemed to be in scope until part way

through the project. The diagram shows specific information exchanges between SecureKey, IBM, IRIS and LCTZ systems. The highlighted areas represent the test scopes described in this test strategy:

1. Card Design
2. Card Manufacturing
3. Card Production
4. Card Production Notification

The following sections describe these categories of testing scope in more detail.

2.2. Card Design

The testing of the card design will be conducted by IRIS, IBM and SecureKey, and will include the following:

- The card has an embedded chip and antenna.
- The chip has been programmed with the chip application in an active state.
- The chip application is configured with the chip data according to the profile.
- The chip antenna has sufficient power for reading chip data.
- The chip data can be read without negative interference from external card features, such as the hologram.
- IBM is able to read chip data using its card production equipment.
- SecureKey is able to read chip data using its card reader equipment.
- SecureKey is able to perform card authentication using its card reader equipment and a test implementation of the SecureKey authentication service.

2.3. Card Manufacturing

The testing of the card manufacturing process, with focus on chip personalization, will be conducted by IRIS and SecureKey, and will include the following:

Chip Personalization (within SecureKey and IRIS's facilities)

- SecureKey generates chip personalization data files.
- SecureKey provides chip personalization data files to IRIS for the purpose of manufacturing cards with active chip applications.
- IRIS provides data files about personalized and damaged cards to SecureKey as part of the card manufacturing reporting.
- SecureKey updates the status of each chip in its chip management system based on the IRIS data files.
- IRIS provides data files about card stock to IBM, including PAN data elements.

IRIS-CMS Technical Integration

- IRIS' SFTP server is configured for and securely implements mutual authentication.
- IRIS and SecureKey create and exchange keys for authenticating to the IRIS' SFTP server.
- CMS authenticates, provides and retrieves data files on IRIS' SFTP server.
- IRIS authenticates, provides and retrieves data files from IRIS' SFTP server.

2.4. Card Production

The testing of the card production process, with focus on additional steps related to the chip, will be conducted by IBM, ICBC and SecureKey, and will include the following:

Card Production Cycle (within IBM's card production facilities)

- IBM creates and exchanges keys with SecureKey for the purpose of encrypting PAN data elements.
- IBM reads the specific chip data from each card as part of the card production cycle.
- IBM determines the PAN data element from card stock data in the case that the chip is unreadable.
- IBM encrypts the PAN data elements read from the chip data.

Card Production Outcome Reporting (with ICBC's card system)

- IBM stores and provides chip data about issued and spoiled cards to ICBC as part of the card production outcomes reporting.
- ICBC stores and processes chip data about issued and spoiled cards.

2.5. Card Production Notifications

The testing of the card production notifications process will be conducted by ICBC, LCTZ, SecureKey and Health, and will include the following:

Issued Card Notifications (with ICBC's card system) (interface BCSC011)

- ICBC provides data files to IAS containing identity, card and chip data for cards that are issued to clients, after they have been produced and mailed by ICBC. Test cases will include:
    - cards issued to clients for the first time, replacement cards, renewal cards, duplicate cards, renewal cards after expiry;
    - combo, standalone photo and non-photo cards;
    - less common cases such as suppressed card addresses, non-Canadian mailing addresses, replacement with different PHN, unknown gender, no given names, long names, replacement of a photo card with a non-photo card; and,
    - data files with a range of low to high record volumes.

Spoiled Card Notifications (with ICBC's card system) (interface BCSC012)

- ICBC provides data files to IAS containing chip data for cards that were spoiled during card production, and thus not issued to clients.
- IAS reads and processes spoiled card data files.

ICBC-IAS Technical integration

- ICBC's FTPS server is configured for and securely implements mutual certificate-based authentication.
- ICBC and LCTZ create and exchange keys for authenticating to the ICBC FTPS server.
- ICBC authenticates and provides data files on its FTPS server on a scheduled basis.
- IAS authenticates and retrieves data files from ICBC's FTPS server on a scheduled basis.

Chip Status Updates (with SecureKey's CMS system)

- IAS creates a MBUN for each new chip issued, to share with CMS.
- IAS provides data files to CMS containing chip status updates, after the card production notification from ICBC and processing within IAS. Test cases will include:
    - cards issued to clients for the first time, replacement cards, renewal cards, duplicate cards, renewal cards after expiry; and,
    - spoiled cards.
- IAS provides data files to CMS containing chip status updates after IAS determines that cards are expired, need to be cancelled, put on hold or released from hold.
- CMS updates the status of each chip in its chip management system based on the IAS data files.
- CMS uses MBUN to transition a cardholder when a card is replaced or renewed.
- CMS decrypts the PAN data elements that IBM encrypted.
- CMS provides a confirmation data file for each card status update file.
- IAS retrieves and processes confirmation data files and report data files.

IAS-CMS Technical integration

- SecureKey's SFTP server is configured for and securely implements mutual authentication.
- LCTZ and SecureKey create and exchange keys for authenticating to the SecureKey SFTP server.
- IAS authenticates, provides and retrieves data files on SecureKey's SFTP server on a scheduled basis.
- CMS authenticates, provides and retrieves data files from SecureKey's SFTP server on a scheduled basis.

Identity Information Updates (with Ministry of Health's HCIM system)

- IAS creates and stores a Health Directed Identifier (HDID) for HCIM.
- IAS encrypts a PHN (SPHN) for HCIM.
- IAS provides data files to Ministry of Health's HCIM system containing identity information updates plus HDID and SPHN, after the card production notification from ICBC and processing within IAS. Test cases will include:
    - cards issued to clients for the first time, replacement cards, renewal cards, duplicate cards, renewal cards after expiry;
    - combo, standalone photo and non-photo cards; and,
    - less common cases such as suppressed card addresses, replacement with different PHN, unknown gender, no given names, long names, replacement of a photo card with a non-photo card.
- HCIM reads and processes identity information updates.
- HCIM decrypts the SPHN to obtain the PHN for a client.
- HCIM sets client records as being card identities.

IAS-HCIM Technical integration

- HCIM is configured for and securely implements mutual certificate-based authentication.
- LCTZ and Health create and exchange keys for authenticating to HCIM.
- IAS authenticates and provides data in web service messages to HCIM.
- HCIM provides response data in web service messages to IAS.

2.6. Out of Scope

This testing strategy document does not cover the following items, however they are (or should be) covered in other testing strategy documents.

- Procedures to monitor and forecast card volumes
- Procedures to order card stock, including consulting with LCTZ, informing SecureKey
- HCIM and R&PB synchronization
- HCIM changes with healthcare points of service
- HCIM identity merges
- Authentication of a card (chip) with IAS, online or at healthcare points of service
- Program reporting and metrics to support benefits evaluation
- Reading card magnetic stripes and bar codes
- Non functional testing types, such as:
    - Security testing
    - Performance testing
    - Usability testing

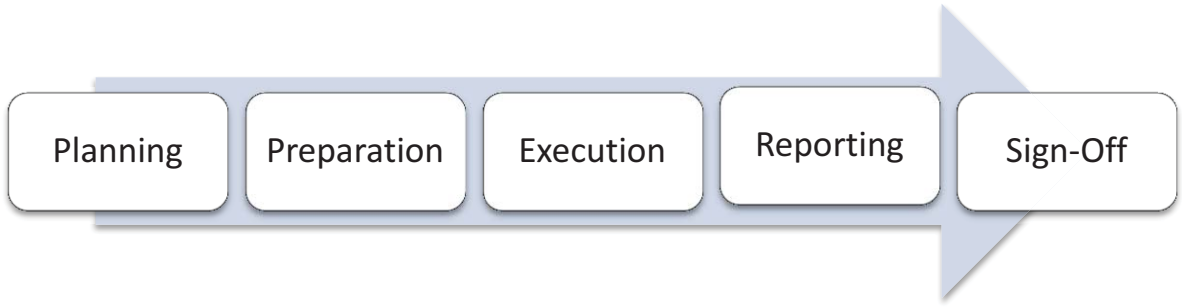
To be discussed further:

- Notifications about investigations (expected to be manual procedures)
- Operational support procedures amongst each organization, including incident mgmt

3. TESTING APPROACH

3.1. Testing Framework

In general, the approach to testing the cards and system integrations is grouped into five phases: planning, preparation, execution, reporting and sign-off.



1. **Planning**. The first phase involves planning the high level testing activities including establishing the scope, approach and timeframe of testing, then documenting the test strategy and plans. During this phase, partners would discuss alignment and then work towards creating more detailed test plans.

2. **Preparation**. The second phase involves preparing for testing, including scheduling specific testing activities and resources, developing test cases and test data, and setting up system testing environments. During this phase, test leads will collaborate to refine the test plans, co-ordinate test cases and test data, and ensure that the testing entry criteria are fulfilled.

3. **Execution**. The third phase is the actual testing effort, conducted with the partners. This involves partner interface testing, end-to-end testing, and defect management and regression testing as needed. During this phase, test leads will collaborate to co-ordinate the execution of tests and test resources. There will be regular and frequent meetings and checkpoints to ensure that all system testing environments and testing resources are aligned.

4. **Reporting**. The fourth phase involves reporting on the results of the testing effort, including documenting action plans to resolve remaining defects. The frequency of reporting while executing the tests will be determined and documented in each test plan.

5. **Sign-off**. The fifth and final phase involves the project sponsors signing off on the testing effort and agreeing that the overall solution is ready to deploy to production operations.

3.2. Assumptions

- Each organization will test their systems adequately internally before the partner integration testing effort;
- Each organization will agree on and share test data during the preparation phase;
- Each organization will co-ordinate test plans;
- Each organization will establish test environments;
- Each organization will have a defect management process and a defect tracking tool to manage their defects;
- Each organization is responsible for reporting their test results; and,
- Each organization is responsible for testing their systems after any code changes and for informing other partners about those changes.

3.3. Testing Types

Throughout the partner integration testing effort, there will be several types of testing conducted by different partners as appropriate:

1. **Physical Card Testing**. The card, chip application and antenna, and the ability to read the chip data will be tested using controlled equipment. This will be tested by IRIS, IBM and SecureKey.

2. **Partner Interface Testing**. Each interface (or small set of interfaces) between two systems (a pair of organizations) is tested by triggering a function within one system that provides data to the other system.

   The following lists the partner interfaces in scope of this testing strategy:
   - SecureKey and IRIS interface about chip personalization
   - IRIS and IBM about card stock with chip data/
   - IBM and ICBC interface about card production outcomes including chip data
   - ICBC and LCTZ interface about issued and spoiled cards
   - LCTZ and SecureKey interface about card status updates
   - LCTZ and Ministry of Health interface about identity information updates

   Additionally there are several partner interfaces between ICBC and HIBC, not described in detail in this testing strategy, but listed for reference purposes and relevant for end to end testing:

   - ICBC and HIBC interface about BCDL and BCID renewal (BCSC001)
   - ICBC and HIBC interface about card qualification check (BCSC002)
   - ICBC and HIBC interface about identity proofing event (BCSC003)
   - ICBC and HIBC interface about card requests and releases (BCSC004)
   - ICBC and HIBC interface about card request updates (BCSC005)
   - ICBC and HIBC interface about combo/photo card returned mail (BCSC006)
   - ICBC and HIBC interface about ICBC address changes (BCSC007)

3. **End to End Testing**. Multiple systems involved in a business process are tested by triggering the first system and allowing the internal processing and information exchanges to occur to all downstream within multiple partners' systems.

   For the card issuance related business processes, all of the above partner interfaces should be tested before beginning the end to end testing. End to end testing is proposed to occur immediately following the ICBC- HIBC joint end to end integration testing.

4. **Regression Testing**. After any changes in the card/chip or systems, tests need to be executed again to confirm that the unchanged portions of the card/chip or systems have not been altered or adversely impacted by the changes.

3.4. Test Cases

Test cases will be derived from design specifications and the testing scope provided in this test strategy document. The test cases will reference to each organization's test cases when needed. A template of a test case is provided in Appendix A.

3.5. Test Data

Test data will be fabricated to support test execution. Test data must have variation to cover all test cases. Furthermore there will be test cases that require a certain volume of test data to represent what will be expected in production operations.

3.6. Testing Environments

Testing will occur in system environments that are not production environments to minimize impact to production operations. Each partner will need to establish a technical testing environment for their respective systems to support the partner integration testing described in this document.

3.7. Testing Entry Criteria

Testing entry criteria are activities that must be completed before partner integration testing activities can begin. The solution architecture is such that some of the partner integration testing may be compartmentalized; that is, that each partner interface can be tested independently before an end-to-end test is performed across all (or most) systems.

The following testing entry criteria are applicable to partner interface testing:

1. Completion of functional system testing
2. Completion of connectivity testing between testing environments
3. Systems are deployed to testing environments
4. Test cases are developed and signed off
5. Test data is available

6. Resources are co-ordinated and ready to execute the test cases

The following testing criteria are applicable to an end-to-end test across multiple partners and systems:

1. Completion of each partner integration independently;
2. Test cases are developed and signed off;
3. Test data is available; and,
4. Resources are co-ordinated and ready to execute the test cases.

3.8. Testing Exit Criteria

Testing exit criteria are results that must be achieved before partner integration testing is complete and ready for sign off. The following testing exit criteria are required for each partner interface test independently, or for an end-to-end test:

1. All test cases must have been executed with documented results;
2. All critical and high severity defects must be resolved and re-tested successfully;
3. All medium and low severity defects must be documented with:
    a. an action plan to resolve if not to be resolved during the testing phase
    b. a documented workaround; and,
4. Agreement with partners that testing is complete.

3.9. Defect Management

Throughout integration testing, defects will be identified. All defects must be logged, tracked and communicated across the partners. Regular and frequent meetings will be scheduled to discuss the defects and their severity, impacts, and whether there are workarounds.

Each logged defect should be logged with the following information:

- The steps to reproduce the defect
- The test case number(s) that revealed to the defect
- Assigned severity and priority
- Action plan to resolve
- Workarounds, if any

The following table lists the classification of the severity of defects that will be used in testing.

Table 1 – Classification of Defect Severity

Severity	Description	Definition
1	Critical	The defect prevents or has the potential to prevent the system or application from meeting the majority of the client requirements. Appropriate where there is widespread system impact to the extent that testing is halted.
2	High	The defect prevents a major function of the system or application from meeting the client requirements and there is no effective work around to meet these requirements. Appropriate for instances where service or delivery has been impacted, although not completely disabled, and there are no workaround procedures available to fix the problem.
3	Medium	The defect prevents a function of the system or application from meeting the requirements, but there is an effective work around to meet these requirements. Appropriate for instances where service or delivery has been impacted, although not completely disabled, and workaround procedures are available to fix the problem.
4	Low	The defect has minimal effect on the system or application meeting the client requirements. Appropriate for errors that are more of a nuisance.

Each organization should agree on the classification of defects. The following matrix of business-system impact (taken from the ICBC-HIBC Joint End to End Strategy document) will help test leads to assess the severity of a defect during test execution. Test leads from each organization should schedule regular defect triage meetings to continuously assess the system and business impacts of the raised defects. Critical defects must be raised and resolved immediately since they impact the testing execution.

Table 2 – Defect Severity Matrix

		Business Impact		
		Low	**Medium**	**High**
System Impact	**Low**	Low	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	Very High

3.10. Test Reporting

During and after the execution of each test case, the results and defects must be recorded. A template of a test report is provided in Appendix B. Test reports will reviewed by test leads, solution leads, development managers and project managers.

4. TESTING SCHEDULE

The following table illustrates the proposed testing schedule for the seven months leading up to production operations.

Table 3 – Testing Schedule

Testing Scope	Partners Involved	Test Type	Cycle	May	June	July	Aug	Sep	Oct	Nov
Card Design	IRIS, IBM, SecureKey	Physical	1	Execution	Reporting					
			2		Execution	Reporting				
Card Manufacturing	SecureKey, IRIS	Partner Interface	1	Preparation	Execution	Reporting				
Card Production	IBM	Physical	1		Preparation	Execution	Reporting			
	IBM, ICBC	Partner Interface	1			Preparation	Execution	Reporting		
Card Production Notifications	ICBC, LCTZ	Partner Interface	1	Planning	Planning Preparation			Execution Reporting		Sign-off
	LCTZ, SecureKey	Partner Interface	1	Planning	Planning Preparation	Execution Reporting				Sign-off
	LCTZ, Health	Partner Interface	1	Planning	Planning Preparation		Execution Reporting			Sign-off
	ICBC, IBM, HIBC, LCTZ, SecureKey, Health	End to End	1						Execution Reporting	Sign-off

5. TESTING ROLES & RESPONSIBILITIES

Table 4 – Testing Roles & Responsibilities

Role	Description	Responsibility
Tester	Any resource that performs tests	• Creates test cases • Performs testing • Documents test results and defects • Escalates defects and testing issues to Test Lead
Test Lead	Primary contact and co-ordinator of testing efforts	• Collaborates with other Test Leads and Solution Leads to define test cases and test data • Co-ordinates testing activities internally and with other Test Leads • Supports testers and monitors test execution • Prepares test reports • Escalates testing issues to Project Manager • Attends defects triage meetings
Solution Lead	Primary contact for solution design	• Collaborates with other Test Leads and Solution Leads to define test cases and test data • Supports Test Leads and monitors testing efforts • Attends defects triage meetings
Project Manager		• Monitors testing efforts • Ensures testing budget and schedule is followed • Assigns tester and test lead resources • Co-ordinates defect resolution with the system development team • Communicates testing progress to Project Sponsors • Escalates issues to Project Sponsors • Attends defects triage meetings
Project Sponsors	Sponsors of project, including testing efforts	• Decision making on testing issues of significant impact • Signs off on testing
Development Manager		• Assigns developers to address defects and create the resolution plan • Communicates defect resolution progress • Co-ordinates defect resolution with the system development team • Attends defects triage meetings

APPENDIX A. TEST CASE TEMPLATE

(under development)

APPENDIX B. TEST REPORT TEMPLATE

Test Report Dashboard

Test cases Categories	Total # of test cases	Total Test cases Passed	Total Test cases Failed	Critical Defects Open	High Defects Open	Medium Defects Open	Low Defects Open	Action Plan / workaround
IAS files from ICBC FTP	3	2	1	0	1	0	0	Does not Exists
IAS pushing files to Secure Key FTP	4	3	1	0	0	1	0	Exists

Defect Summary Report

Defect	Description	Action	Assigned to	Due on
101	IAS can't push 4 files to the secure Key FTP server due to access denied	SK and IAS Technical teams to check the FTP configurations	John Techie	Oct 1, 2012
102	Xxx	Xxx	Xxx	xxx

BC Services Card Project

SecureKey Integration Test Plan

DRAFT

Version: 1.0
July 18, 2012

Document Information

This is a point-in-time version of a document. Please contact the author or the person who issued this document (listed below) if you are in any doubt about the currency of this document.

Document title	SecureKey Integration Test Plan
Document file name	SecureKey Integration Test Plan V1.0.docx
Revision number	1.0
Issued by	LCTZ
Issue Date	July 18, 2012
Status	Draft

Document Purpose and Intended Audience

This document describes a more detailed test plan from Ministry of Labour, Citizens' Services and Open Government (LCTZ)'s perspective relevant to the initial release of the BC Services Card program.

The scope of this document is focused on the testing related to the functions and information exchanges for integrating IAS and SecureKey systems.

This document is intended to facilitate alignment of effort and scope of the testing effort leading up to implementing the system into production in November, 2012.

Document References

The following documents are related to this document.

1. BCSC ICBC-HIBC Joint End to End Test Strategy
2. BCSC IAS and CMS Interface Design Specification
3. LCTZ Partner Integration Testing Strategy

Document Version History

Version	Revision Date	Author	Summary of Changes	Changes Marked?
1.0	July 18, 2012	Jason Owens	Initial Draft	

Document Contents

1. TESTING SCOPE

The scope of this document is focused on functional integration testing between the LCTZ IAS system and SecureKey systems. Specifically, the following areas are targeted as “in scope” in the context of this test plan:

- Data Transfer Interface testing between IAS and SecureKey’s SFTP server
- Performance and Volume testing of IAS as it pertains to the SecureKey interface
- Security/Authentication testing of IAS as it pertains to the SecureKey interface
- Draft internal procedure development for activities related to interactions with SecureKey
- Task Information Management (TIMS) application testing for issue workflow

A detailed breakdown of each of the above items can be found in section 3.1 of this document (“Testing Types”).

1.1. Out of Scope

The following items are considered out of scope of this plan:

- Procedure testing (for example, exchange of phone numbers and procedure for contacting in the case of technical/connectivity issues). Procedures will be executed and tested as part of the “End-to-End” testing phase.
- Penetration testing – this will be conducted by a third party; details still being finalized.
- Failover/Recovery testing – this will also be tested and executed as part of the “End-to-End” testing phase.
- Integration testing with HCIM and ICBC

2. TESTING ENTRY AND EXIT CRITERIA

2.1. Entry Criteria

The following items are assumed to be in place prior to commencement of the integration testing phase:

1. Connectivity testing complete. End points for both IAS and SecureKey systems discovered; appropriate exchanges of keys and credentials have occurred. All routes (firewall ACLs etc) established and confirmed.
2. Test tools identified and configured (repositories created etc).
3. Test cases are developed and signed off
4. Test data is created and available for testing
5. Resources identified, knowledge transfer/training completed.
6. Test / Pre-Prod environment infrastructure configured and available for both IAS and SecureKey systems.
7. Testing approach and schedule confirmed and aligned between both parties.

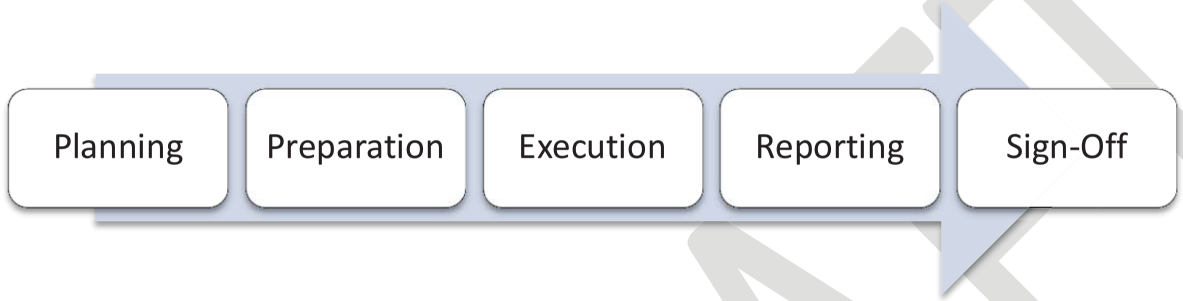
2.2. Exit Criteria

The completion of the following items is necessary in order to consider the integration testing phase “complete”:

- All test cases must have been executed with documented results;
- All severity 1 and 2 defects are fixed and retested
- All outstanding defect review meetings held.
- Defect triage complete; “Testing Checkpoint Meeting” held. All defects either repaired or determined “low risk” and signed off by management.
- Test Report created and distributed to all parties.
- Final Integration Testing Sign-Off meeting held; signed off by SecureKey, test leads, and management.

3. TESTING APPROACH

The testing approach for the IAS – CMS integration testing is derived from the testing approach defined in the LCTZ Partner Integration Testing Strategy where testing activities are grouped into five phases: Test planning, Test Preparation, Test Execution, Test Reporting and sign-off.



3.1. Testing Types

3.1.1. Data Transfer Interface

Chip Status Updates (with SecureKey's CMS system)

- IAS creates a MBUN for each new chip issued, to share with CMS.
- IAS provides data files to CMS containing chip status updates, after the card production notification from ICBC and processing within IAS. Test cases will include:
  - cards issued to clients for the first time, replacement cards, renewal cards, duplicate cards, renewal cards after expiry; and,
  - spoiled cards.
- IAS provides data files to CMS containing chip status updates after IAS determines that cards are expired, need to be cancelled, put on hold or released from hold.
- CMS updates the status of each chip in its chip management system based on the IAS data files.
- CMS uses MBUN to transition a cardholder when a card is replaced or renewed.
- CMS decrypts the PAN data elements that IBM encrypted.
- CMS provides a confirmation data file for each card status update file.

- IAS retrieves and processes confirmation data files and report data files.

IAS-CMS Technical integration
- IAS provides and retrieves data files on SecureKey's SFTP server on a scheduled basis.
- CMS provides and retrieves data files from SecureKey's SFTP server on a scheduled basis.

3.1.2. Performance testing

Using data that is seeded and mocked to simulate the ICBC process and with defined performance baselines (tbd); complete the following;
- Verify throughput on network
- Check overall transaction response times
- Check the capacity of the system
- Verify Database access times
- Check resource utilization under normal loads and stress loads
- Test the Production environments before going Live.
- Capture all problems and issues related to performance as early as possible.

3.1.3. Security testing - requirements in the IAS-CMS design spec

- SecureKey's SFTP server is configured for and securely implements mutual authentication.
- LCTZ and SecureKey create and exchange keys for authenticating to the SecureKey SFTP server.
- LCTZ / IAS server **authenticates** successfully to SecureKey SFTP server
- Confirm that files are encrypted as expected during transfer to SecureKey
- Confirm that SecureKey is able to un-encrypt the files and the data is intact.

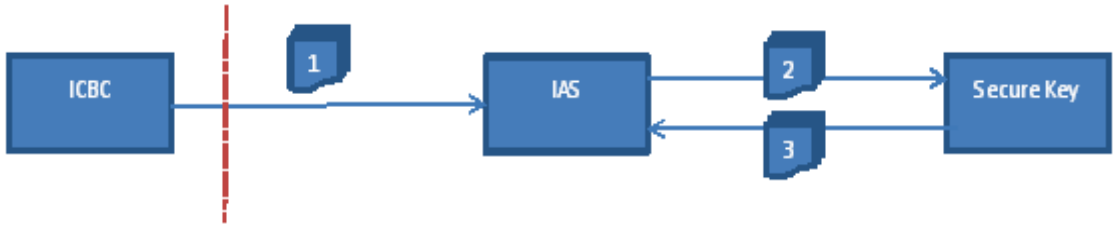
3.2. Test Cases

The following are the high level list of test cases. As appropriate each test case will include steps to validate issue workflow, security protocols and confirmation reporting.

ID #:	Title:
ITSK-01	Active New Card / Registration (PAN)
ITSK-02	Active additional card (PAN)
ITSK-03	Replace Card
ITSK-04	Renew before expiry
ITSK-05	Replace after expiry
ITSK-06	Spoiled Cards
ITSK-07	Expired Cards
ITSK-08	Performance (internal execution)
ITSK-09	Performance (external interface)
ITSK-10	Security/Encryption
ITSK-11	Volume Testing
ITSK-12	Edge/Error Cases
ITSK-13	Reports (Card Status, Restores and Support)
ITSK-14	Suspend
ITSK-15	Un-suspend

3.3. Test Data

The test data is seeded to simulate the ICBC data file. Files “1” will not be sent by ICBC. Therefore, the file will be created by the IAS testing team and will be processed in IAS to produce CMS notification files which are files “2”. Files “3” are the reports and the confirmation files that Secure Key will send to IAS after receiving files “2”.



3.4. Test Tools

The following tools have been identified as required to execute the Integration Testing:

- SharePoint 2010 as the Issues tracking tool.
- An FTP client (pre-loading ICBC interface) – FileZilla, WSFTP, etc.
- An XML editor with syntax highlighting, node matching – Textpad, Notepad++ etc.
- An Oracle SQL development tool – SQL Developer, PL/SQL, Toad etc.
- Access to WebMethods Integration server.
- Access to My WebMethods site.

3.5. Testing Environments

Testing will be performed in a dedicated pre-production environment designed to closely mimic the infrastructure and capabilities of the production environment. The environment will be frozen during the test period. Any changes to configuration of the test environment are controlled through the test team.

3.6. Test Deliverables

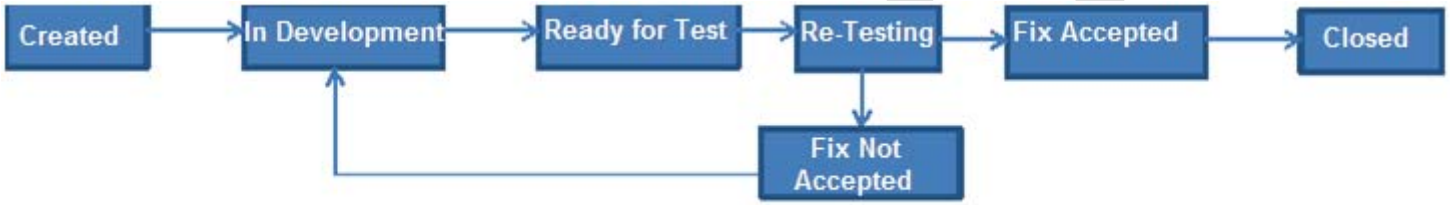
The following deliverables are in scope of the test plan. Appropriate templates are available in the appendix.

- Test Plan
- Test Cases
- Test Data
- Defect Reports
- Test/Result Report

3.7. Defect Management

Throughout integration testing, defects will be identified. All defects must be logged, tracked and communicated between the IAS and the SecureKey testing teams. Regular and frequent meetings will be scheduled to discuss the defects and their severity, impacts, and whether there are workarounds.

The IAS defects will be logged in SharePoint 2010. The life cycle of the defect is illustrated below:



Each defect should be logged with the following information:

- The steps to reproduce the defect
- The test case number(s) that revealed to the defect
- Assigned severity and priority
- Action plan to resolve
- Workarounds, if any

The following table lists the classification of the severity of defects that will be used in testing.

Table 1 – Classification of Defect Severity

Severity	Description	Definition
1	Critical	The defect prevents or has the potential to prevent the system or application from meeting the majority of the business requirements. Appropriate where there is widespread system impact to the extent that testing is halted.

2	High	The defect prevents a major function of the system or application from meeting the business requirements and there is no effective work around to meet these requirements. Appropriate for instances where service or delivery has been impacted, although not completely disabled, and there are no workaround procedures available to fix the problem.
3	Medium	The defect prevents a function of the system or application from meeting the requirements, but there is an effective work around to meet these requirements. Appropriate for instances where service or delivery has been impacted, although not completely disabled, and workaround procedures are available to fix the problem.
4	Low	The defect has minimal effect on the system or application meeting the business requirements. Appropriate for errors that are more of a nuisance.

4. TESTING SCHEDULE

The following table illustrates the proposed testing schedule for the SecureKey integration testing.

Tasks	Start Date	Due Date
SK Testing		
SK Test Planning		
SK Test Preparation		
Define the SK testcases	03-Jul	06-Jul
Review the high level test cases with SK	04-Jul	06-Jul
Create the details of the testcases	09-Jul	13-Jul
Seed test data	09-Jul	13-Jul
Smoke test the pre-prod environment	12-Jul	13-Jul
Testing tools setup	09-Jul	13-Jul
Testcases walkthrough, knowledge transfer	10-Jul	12-Jul
SK Integration readiness	13-Jul	13-Jul
SK Test Execution		
SK Integration testing kick-off	16-Jul	17-Jul
Attend daily scrums	16-Jul	27-Jul
Execute test cases	16-Jul	27-Jul
Perform regression test	16-Jul	27-Jul
Attend Defect Review meetings	16-Jul	27-Jul
Testing Completion checkpoint	26-Jul	27-Jul
SK Test Reporting		
Create Test report	30-Jul	31-Jul
SK Integration testing sign-off	01-Aug	02-Aug

5. TESTING ROLES & RESPONSIBILITIES

Test Lead

- Develop Test Plan, test cases and test schedule
- Overall accountability for planning and execution of testing
- Escalation of issues or problems to testing team and/or management
- Managing testing risks and escalation to the project team as needed
- Reviewing testing deliverables and artefacts for completeness
- Coordinate test planning
- Provide knowledge transfer to testing resources
- Approve implementation of new functionality/code change to the test environment
- Tracking application test progress
- Logging technical issues in defined tool
- Development of final test report
- Generate test data Facilitate daily scrums with the testers
- Report testing status to management

Testers

- Participate in test case development/knowledge transfer activities
- Execute tests
- Log defects to the defect tracking tool as defined
- Document all test results
- Identify ties ins to procedures development/updates
- Escalate issue to the test lead

Technical Support

- Set up application testing environment
- Maintains application within the test environment
- Investigate and fix defects related to application
- Provide support for testers throughout test cycle

Project Management

- Review and approve test plan document
- Ensure that adequate resources are available to perform testing
- Address escalated issues and concerns as a priority to ensure that timelines are not impacted

6. ASSUMPTIONS AND RISKS

The following assumptions and risks will impact the capability to execute testing as scheduled.

6.1. Assumptions

- Adequate Resources are available to participate
- Partners are ready to perform testing according to the defined schedule
- A defect management process and a defect tracking tool to manage defects

6.2. Risks

- Resources availability changes (labour disruptions, illness, etc.)
- Infrastructure readiness
- Partner schedule changes
- Corporate infrastructure stability

APPENDIX A. GLOSSARY

Term	Description
PAN	Personal Account Number
MBUN	Meaningless But Unique Number – a form of directed identifier used in communication between IAS and SK systems; associated in SK system with the card PAN

APPENDIX B. TEST CASE TEMPLATE

Test Case ID -	**TSK - 01**
Test Case Name:	**Active New Card / Registration (PAN)**
Description/Objective	**Creation of a new identity record in IAS results in a <activate new card> request being sent to Secure Key. Secure Key validates and processes the request, resulting in an activated state for the PAN (Services Card chip number). Secure Key generates a confirmation file indicating the successful activation.**
Tools	**SFTP Client, Oracle SQL Query Tool, XML Editor, Integration Server, My WebMethods, Secure Access Gateway (Vmware client)**
Data File	s 15
Name of Tester	**John A Smith**
Date	**18-Jul-12**

Step #	Steps	Expected Results	Actual Results	Comments	Defect #	Procedure Reqd?

APPENDIX C. TEST REPORT TEMPLATE

Defect Summary Report

Defect	Description	Action	Assigned to	Due on
101	IAS can't push 4 files to the secure Key FTP server due to access denied	SK and IAS Technical teams to check the FTP configurations	John Techie	Oct 1, 2012
102	Xxx	Xxx	Xxx	xxx

Page 179 redacted for the following reason:
- -
S 15