



Ref: 97849

February 26, 2013

Mr. Jaime Shapiro  
President  
SecureKey Technologies Inc.  
Suite 2900, 199 Bay St.  
PO Box 366  
Toronto, Ontario  
M5L 1G2

Dear Jaime Shapiro:

**Re: SecureKey Notice of Readiness Production Feb 11 2013**

Subject to the conditions and qualifications below, the Province hereby provides this notice that Card Management Services have been fully accepted by the Province in accordance with the provisions of Section 6 of Schedule 3.2 of the Master Services Agreement entered into by the Province and SecureKey Technologies Inc. ("SecureKey"), dated as of April 13, 2012 (the "MSA"). As per Milestone 8 in Section 3(c) of Appendix 2.2 to Schedule 1.5 of the Card Management and Authentication Services Statement of Work (SOW) under the MSA, Card Management Services have been fully accepted by the Province and are in full operation, and the Service Levels for such Services are in effect.

For greater certainty, this acceptance of Card Management Services (CMS) includes:

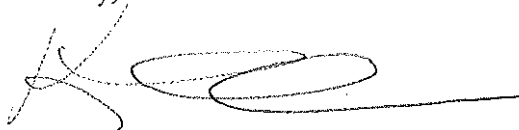
1. The following Test Components described in detail in Appendix 2.2 to Schedule 1.5 of CMS SOW under the MSA:
  - (i) Personalization and authentication using test cards
  - (ii) Personalization and authentication using production cards
  - (iii) Services Card Status updates
2. The four key elements of CMS (i.e. PAN Management and Assignment, Services Card Personalization, Card Management Database, Services Card Status Updates), as described in Section 1 of Appendix 2.2 to Schedule 1.5 of CMS under the MSA

subject to the following conditions and qualifications:

- A defect has been identified in how CMS handles card status reports related to error situations (Issue #7366 – “Sometimes CMS generates Zero byte card status updates Reports”). This defect was addressed as a Failure Notice in the Province’s letter to SecureKey dated February 8, 2013 with respect to such Test Component. SecureKey must address by March 31, 2013, then notify the Province so a re-test can be performed. Failure to meet this deadline will be deemed a Service Level Failure as per the provisions of Section 6 of Schedule 3.4 of the MSA (Service Levels) as described under Appendix 2.5 to Schedule 1.5 (Service Levels for SOW Services).

The Province looks forward to working with SecureKey as CMS is now in full production operation, and continuing to work on the Authentication Services and Terminal Equipment Services as described in Schedule 1.5 to the MSA.

Sincerely,



Kevena Bamford  
Executive Director  
Provincial IDIM Program

pc: Andre Boysen, SecureKey Technologies Inc.  
Heather Neale, SecureKey Technologies Inc.  
Chris Chapman, SecureKey Technologies Inc.  
Ian Bailey, Ministry of Citizens’ Services and Open Government  
Patricia Wiebe, Ministry of Citizens’ Services and Open Government  
Jeremy Moss, Ministry of Citizens’ Services and Open Government



Ref: 99929

October 22, 2013

Mr. Jaime Shapiro  
President  
SecureKey Technologies Inc.  
Suite 2900 - 199 Bay St.  
PO Box 366  
Toronto, Ontario  
M5L 1G2

Dear Jaime Shapiro:

**Re: SecureKey Notice of Readiness October 15, 2013**

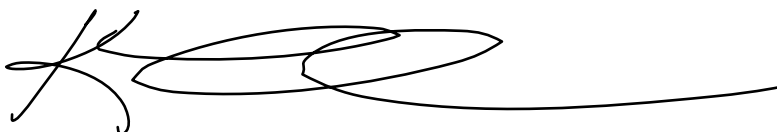
The Province hereby provides this Notice of Acceptance for the following Test Components of the Authentication Services in accordance with the provisions of Section 3 of Schedule 3.2 of the Master Services Agreement entered into by the Province and SecureKey Technologies Inc. ("SecureKey"), dated as of April 13, 2012 (the "MSA"), which the Province and SecureKey intend to amend by Change Order #CO-1 currently being negotiated.

The Province hereby:

- 1) Accepts the following Test Components for purposes of Schedule 3.2 of the MSA (described in detail in Appendix 2.3 to Schedule 1.5 of the Authentication Services SOW under the MSA):
  - a. Authentication with USB terminal
  - b. User Interface
  - d. Security
- 2) Accepts the readiness for Acceptance Testing of the following key elements of the Authentication Services, as described in Appendix 2.3 to Schedule 1.5 of the Authentication Services SOW under the MSA:
  - a. EMV Cryptographic Authentication
  - b. User Interface
  - c. Security Specifications

- 3) Accepts for Acceptance Testing that:
  - a. USB Authentication Tokens and prototype USB Counter Devices are available for testing, except to the extent SecureKey is making efforts to correct Deficiencies identified by the Province with respect to USB Authentication Tokens so that the Province can resume Acceptance Testing with respect to such tokens.
  - b. The Supplier Authentication Services will integrate with the Province using the JSON protocol and data formats.
  - c. SecureKey's Security documentation has been made available.
- 4) Acknowledges receipt of the following documents from SecureKey:
  - a. Card Authentication Test Plan v0.3
  - b. BC Regression Test Exit Report v0.2
- 5) Acknowledges receipt from SecureKey of:
  - a) User acceptance test environment that supports multiple test instances to enable the Province to test its own different identity environments
  - b) Additional CMS test environment
- 6) Acknowledges that:
  - a. the reporting design is outstanding with completion pending design review sessions in accordance with the MSA.
  - b. Performance Testing results will be made available to the Province on November 25, 2013.

Sincerely,



Kevena Bamford  
Executive Director  
Provincial IDIM Program

pc: Andre Boysen, SecureKey Technologies Inc.  
Heather Neale, SecureKey Technologies Inc.  
Chris Chapman, SecureKey Technologies Inc.  
Ian Bailey, Ministry of Technology, Innovation and Citizens' Services  
Patricia Wiebe, Ministry of Technology, Innovation and Citizens' Services  
Jeremy Moss, Ministry of Technology, Innovation and Citizens' Services

## HOSTING FAILOVER AGREEMENT

THIS HOSTING FAILOVER AGREEMENT is made as of July 10, 2012 (the “**Effective Date**”) between Q9 NETWORKS INC. (“**Hosting Provider**”), an Ontario corporation, having an address at 77 King Street West, Suite 4400, Toronto, Ontario M5K 1J3 (Fax: 416-362-7001), SECUREKEY TECHNOLOGIES INC. (“**Supplier**”), an Ontario corporation, having an address at 199 Bay Street, Suite 2900, PO Box 366, Toronto, Ontario M5L 1G2 (Fax: 416-214-9895) and HER MAJESTY THE QUEEN IN RIGHT OF THE PROVINCE OF BRITISH COLUMBIA (the “**Province**”), as represented by the Minister of Labour, Citizens’ Services and Open Government, having an address at 4000 Seymour Place, Victoria, British Columbia V8X 4S8 (attention: Ministry of Labour, Citizen Services and Open Government, Technical Services Division) (Fax: 250-387-1940).

### BACKGROUND:

- A. Supplier and the Province have entered into a Master Services Agreement made as of April 13, 2012 (as may be amended from time to time, the “**MSA**”) under which Supplier will provide certain chip-based identity card management and authentication services to the Province (the “**MSA Services**”).
- B. Supplier has advised Hosting Provider that it is a key service provider of Supplier approved by the Province (as a subcontractor under the MSA) to provide hosting of Supplier’s live production and commercial environments and certain related services (“**Hosting Services**”) which Supplier has advised Hosting Provider are used by Supplier to support Supplier’s provision of the MSA Services under the MSA.
- C. Hosting Provider and Supplier have entered into an Internet Infrastructure Services Agreement made as of October 21, 2011 under which Hosting Provider will provide Hosting Services to the Supplier (the “**Hosting Contract**”).
- D. It is a requirement of the MSA that the Province, Supplier and Hosting Provider enter into an agreement governing: (I) the rights of the Province to ensure the continuity of the Hosting Services in accordance with the MSA; and (II) certain other matters required by the MSA.

NOW THEREFORE, in consideration of the mutual covenants and agreements contained in this Agreement, Hosting Provider, Supplier and the Province (each, a “**Party**”) agree as follows.

## 1 CONTINUITY OF HOSTING SERVICES

- 1.1 Amendment and Termination of Hosting Contract. Supplier will not amend (whether by agreement or otherwise) or terminate, without the prior written approval of the Province, the Hosting Contract, or any term or condition therein, in a manner that would deprive the Province of the protections provided to it under this Agreement. Hosting Provider will provide written notice to the Province, concurrent with any notice provided to Supplier of any termination of the Hosting Contract or termination or suspension of the provision of the Hosting Services in either case effected by the Hosting Provider unilaterally. Notwithstanding the effect on the Province, nothing in this Section 1.1 shall serve to limit the rights afforded to the Hosting Provider in the Hosting Contract to terminate or suspend the provision of the Hosting Services (subject only to any applicable notice and cure periods as prescribed in the Hosting Contract) and to enter into amendments with the Supplier to the Hosting Contract from time to time as requested by Supplier.

- 1.2 Breach of Hosting Contract by Supplier. Hosting Provider will provide a copy of any notice of breach of the Hosting Contract by Supplier to the Province concurrently with the provision of such notice to Supplier of such breach, including details with respect to the nature of the breach. The Supplier acknowledges and agrees that the Hosting Provider shall be permitted to respond to any inquiry directly from the Province with respect to the subject breach and to confirm what is required to remedy such breach, including confirming whether or not remedy is possible in the circumstances and to assist the Province in determining whether any such breach can be cured by the Province.
- 1.3 Non-payment by Supplier under Hosting Contract. The Province will be entitled to remedy any non-payment of fees or other amounts payable by Supplier to Hosting Provider under the Hosting Contract. Hosting Provider agrees to accept any such payments made by the Province and to treat any such payments as curing any failure by Supplier to pay any amounts under the Hosting Contract when due and payable on a dollar for dollar basis.
- 1.4 Conditional Right of the Province to Directly Instruct Hosting Provider. In the event Supplier (a) ceases to do business as a going concern, is unable to pay its debts as they become due, files or becomes the subject of a petition in bankruptcy, appoints a receiver, acquiesces in the appointment of a receiver or trustee, becomes insolvent, makes an assignment for the benefit of creditor, goes into liquidation or receivership or otherwise loses legal control of its business and (b) has no functioning management or operational capability, the Province will notify Hosting Provider of such event and, upon Hosting Provider's receipt of such notice, the Province will be entitled to communicate and otherwise deal with Hosting Provider directly (including by providing direct instructions to Hosting Provider as if the Province were its direct customer) to the extent necessary to ensure that Supplier continues to receive Hosting Services from Hosting Provider in accordance with the Hosting Contract despite such event. Notwithstanding the foregoing, if Hosting Provider determines, acting reasonably, that compliance with any instructions provided by the Province under this Section 1.4 would or could result in additional liability to Hosting Provider, Hosting Provider may require as condition of compliance with such instructions that the Province enter into an agreement with Hosting Provider that addresses such liability to the reasonable satisfaction of Hosting Provider. For greater clarity, to the extent that the Supplier's environment within Hosting Provider's facility is continuing to operate, then it is reasonable for Hosting Provider to conclude that additional liability could ensue given that Supplier is no longer able to meet its obligations pursuant to the Hosting Contract, and therefore, Hosting Provider shall be entitled to request that the Province enter into an agreement with this Hosting Provider. If any such agreement is required and the Province elects to proceed with the negotiation of the agreement, Hosting Provider and the Province will negotiate the terms and conditions of such agreement in good faith and in a timely manner. Notwithstanding the foregoing, nothing in this Section 1.4 will require Hosting Provider to not comply with any applicable laws or any court order or judgment binding on Hosting Provider. For purposes of this Section 1.4, Supplier will, without limitation, be deemed to have no functioning management or operational capability if: (i) Supplier has been notified in writing by Hosting Provider that it has failed to perform any of its material obligations under the Hosting Contract (including any failure to make any required payments under the Hosting Contract, notwithstanding whether the Province has remedied such non-payments in accordance with Section 1.3) and such failure has not been cured by Supplier within the cure period specified in the Hosting Contract; (ii) such failure has resulted from Supplier having no functioning management or operational capability, as determined by the Province acting reasonably; and (iii) Supplier does not respond within five (5) business days to any of the requests by either the Province or Hosting Provider to Supplier for confirmation of Supplier's management and operational capability using each of the following contact methods: (A) the Supplier address and fax number specified on the first page of this

Agreement; (B) the Supplier contact methods listed on Supplier's website [www.securekey.com](http://www.securekey.com); and (C) the following officer/director contact information: for Jaime Shapiro, [jaime.shapiro@securekey.com](mailto:jaime.shapiro@securekey.com) and [greg.wolfond@securekey.com](mailto:greg.wolfond@securekey.com) and s 22 and for Greg Wolfond, For clarity, unless Province agrees otherwise in a separate written agreement with the Hosting Provider as described above in this Section 1.4, the Province is not assuming any obligations or liability of Supplier under the Hosting Contract pursuant to this Agreement.

- 1.5 Access Rights. Hosting Provider hereby confirms that Section 3 of the Hosting Contract provides that, subject to compliance with all applicable security, safety and authorization procedures, access to the Supplier's dedicated environment within the Hosting Provider's data centre facility where Supplier has contracted for capacity (the "**Space**") shall be available twenty-four (24) hours per day and seven (7) days per week to employees and agents of the Supplier whom the Supplier has authorized to have access to the Space in accordance with Hosting Provider's operational procedures and data centre rules and guidelines and which may include representatives of the Province.

## **2 TERM AND TERMINATION**

- 2.1 Term. This Agreement will begin on the Effective Date and will continue until the earlier of: (a) termination or expiry of the MSA and the completion of all transition assistance services provided by Supplier to the Province relating to the Hosting Services, provided that Supplier shall have notified Hosting Provider of the effective date of such termination; and (b) the termination of the Hosting Contract.
- 2.2 Survival. Neither the expiration nor the earlier termination of this Agreement will release any of the Parties from any obligation or liability that accrued prior to the expiration or termination. The provisions of this Agreement requiring performance or fulfilment after the expiration or earlier termination of this Agreement, including Section 1.5 and this Section 2.2, such other provisions as are necessary for the interpretation thereof, and any other provisions hereof, the nature and intent of which is to survive termination or expiration of this Agreement, will survive the expiration or earlier termination of this Agreement.

## **3 MISCELLANEOUS**

- 3.1 Interpretation. The division of this Agreement into Sections and the insertion of a table of contents and headings are for convenience of reference only and do not affect the construction or interpretation of this Agreement. The terms "hereof", "hereunder" and similar expressions refer to this Agreement and not to any particular Section or other portion hereof. Unless something in the subject matter or context is inconsistent therewith, references herein to Sections are to Sections of this Agreement. In this Agreement, words importing the singular number only include the plural and vice versa and words importing any gender include all genders. The term "including" means "including without limiting the generality of the foregoing". A definition applies to other forms of the word.
- 3.2 Entire Agreement. This Agreement constitutes the entire agreement between the Parties with respect to the subject matter hereof and cancels and supersedes any other understandings and agreements between the Parties with respect thereto. There are no representations, warranties, terms, conditions, undertakings or collateral agreements, express, implied or statutory, between the Parties other than as expressly set out in this Agreement.


- 3.3 Amendment. Except as otherwise expressly permitted or specified herein, this Agreement will not be amended except by a written agreement that: (a) is signed by the authorized signing representatives of each of the Parties; and (b) expressly states that it is intended to amend this Agreement.
- 3.4 Severability. If any provision of this Agreement is determined by any court of competent jurisdiction to be illegal or unenforceable, that provision will be severed from this Agreement and the remaining provisions will continue in full force and effect so long as the economic or legal substance of the transactions contemplated hereby is not affected in any manner materially adverse to either of the Parties.
- 3.5 Relationship of the Parties. Except where this Agreement expressly provides to the contrary, nothing contained in this Agreement will be deemed or construed by the Parties, or by any third party, to create the relationship of partnership or joint venture or a relationship of principal and agent, employer-employee, master-servant, or franchisor-franchisee between any of the Parties and no provision contained herein will be deemed to create any relationship between any of the Parties other than the relationship of independent parties contracting for services.
- 3.6 Assignment. This Agreement and the rights granted hereunder will not be assigned by Supplier without the prior written consent of the Province, not to be unreasonably withheld. The Province may assign this Agreement at any time; provided, however, that prior notice of assignment is provided to Hosting Provider and Supplier. Hosting Provider may assign and transfer this Agreement to any entity to which it assigns the Hosting Contract and upon such assignment shall be released from any further obligation hereunder, provided Hosting Provider shall notify Supplier and the Province of any such assignment in writing concurrently with its notification to the Supplier as and when required pursuant to the Hosting Contract.
- 3.7 Benefit of the Agreement. This Agreement will enure to the benefit of and be binding upon the respective successors and permitted assigns of the Parties.
- 3.8 Time is of the Essence. Time is of the essence of this Agreement and each provision herein.
- 3.9 Notices. Any notice contemplated by this Agreement, to be effective, must be in writing and delivered as follows: (a) by fax to the addressee's fax number specified on the first page of this Agreement, in which case it will be deemed to be received on the day of transmittal unless transmitted after the normal business hours of the addressee or on a day that is not a business day, in which cases it will be deemed to be received on the next following business day; (b) by hand to the addressee's address specified on the first page of this Agreement, in which case it will be deemed to be received on the day of its delivery; or (c) by prepaid post to the addressee's address specified on the first page of this Agreement, in which case if mailed during any period when normal postal services prevail, it will be deemed to be received on the fifth business day after its mailing. Any Party may from time to time give notice to the other Parties of a substitute address or fax number, which from the date such notice is given will supersede for purposes of this Section any previous address or fax number specified for the Party giving the notice.
- 3.10 Public Disclosures. All media releases, public announcements or external disclosures of any nature by Hosting Provider or Supplier relating to this Agreement or its subject matter will be coordinated with and must be approved in advance by the Province prior to the release thereof.
- 3.11 Further Assurances. The Parties agree to do all things and to execute all further documents as may reasonably be required to give full effect to this Agreement.



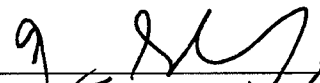
- 3.12 Governing Law. This Agreement will be governed by and construed in accordance with the laws of the Province of British Columbia and the laws of Canada applicable therein.
- 3.13 Counterparts and Electronic Execution. This Agreement may be executed in any number of counterparts, each of which will be deemed to be an original, and all of which taken together will be deemed to constitute one and the same instrument. Delivery of an executed signature page to this Agreement by any Party by electronic transmission will be as effective as delivery of a manually executed copy of the Agreement by that Party.

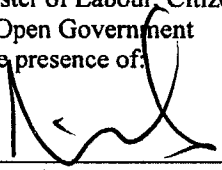
EXECUTED by the Parties as of the Effective Date.


**Q9 NETWORKS INC.**

By:  c/s  
Name: Victoria Coombs  
Title: General Counsel & Secretary

**SECUREKEY TECHNOLOGIES INC.**

By:  c/s  
Name: Jaime Shapiro  
Title: President

SIGNED on behalf of Her Majesty )  
the Queen in right of the Province )  
of British Columbia by a duly )  
authorized representative of the )  
Minister of Labour, Citizens' Services )  
and Open Government )  
in the presence of: )  
 )  
(Witness) )

  
For the Minister  
DAVE NIKOLESSIN  
CIO



July 26, 2012

CONFIDENTIAL

Securekey Technologies Inc.  
Suite 2900, PO Box 366,  
Toronto, Ontario  
V8X 4S8

Attention: Jaime Shapiro

Dear Mr. Shapiro:

**Re: Master Services Agreement between Securekey Technologies Inc. (the "Supplier") and Her Majesty the Queen in Right of the Province of British Columbia, as represented by the Minister of Labour, Citizens' Services and Open Government (the "Province") made as of April 13, 2012 (the "MSA")**

In connection with the MSA and the Hosting Failover Services Agreement dated as of July 10, 2012 entered into between the Supplier, the Province and Q9 Networks Inc. (the "**Hosting Failover Agreement**") pursuant to Section 12.10 of the MSA, the Province would like to clarify and confirm with the Supplier the approach and design specifications for the Transition File and the related measures to ensure continuity of the Services in accordance with Sections 12.6 to 12.11 (inclusive) of the MSA.

Except as otherwise specified in this letter agreement, capitalized terms not defined in this letter agreement have the same meanings given to them in the MSA.

After having completed discussions with respect to the above referenced matters, the Province and the Supplier acknowledge and agree as follow:

1. As part of the Services, the Supplier will comply with all of its obligations under the document titled "BC Services Card Transition Design Specification" attached to this letter agreement as Exhibit A (the "**Transition Specification**"), including, without limitation, to:
  - (a) produce, maintain, backup, encrypt, update, and provide the Province with access to the Transition File and the Tracking File (as defined under the Transition Specification) in accordance with the Transition Specification;
  - (b) generate, update, and make available to the Province the Encryption Keys in accordance with the Transition Specification;

- (c) conduct all necessary testing as specified in the Transition Specification; and
  - (d) provide the Province with assistance in accessing the Transition File from the Hosting Provider in accordance with the Transition Specification.
2. The Supplier agrees that the Transition File will at all times be stored with the Hosting Provider (i.e. Q9 Networks Inc.) on a server hosted by the Hosting Provider and located in the Space (as defined in the Hosting Failover Agreement).
  3. Under its agreement with the Hosting Provider (as confirmed in the Hosting Failover Agreement), the Supplier has the right to designate a third party representative (the "Access Representative") who will be given access by the Hosting Provider to the cabinet holding the particular server and any other hosted infrastructure used to provide the Services (including the server upon which the Transition File is stored), which will be located within the Space. The Supplier will appoint each individual that the Province designates in writing to the Supplier as an Access Representative. The Province may change the persons designated to be its Access Representatives from time to time upon written notice to the Supplier. The Province hereby designates the individuals listed in Exhibit B as its initial Access Representatives.
  4. The Supplier will promptly notify the Province in writing of any notices it receives from the Hosting Provider with respect to any amendment or termination of the Hosting Contract or suspension of the services provided by Hosting Provider under the Hosting Contract that would deprive the Province of its protections under the MSA and will provide such details related to any such amendment, termination of suspension as may be reasonably requested by the Province.
  5. Upon the escrow of the Encryption Keys and the Failover Security no longer being required under the terms and conditions of the MSA, the Province will cooperate with the Supplier with respect to all actions required to terminate the applicable Escrow Agreement and cancel the Failover Security.

If you are in agreement with the foregoing, please return a copy of this letter agreement executed by the Supplier. Execution of this letter agreement by the Supplier will confirm that the Supplier accepts and agrees to be bound by the provisions of this letter agreement.

Sincerely,

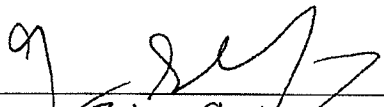
**Her Majesty the Queen in Right of the Province  
of British Columbia, as represented by the  
Minister of Labour, Citizens' Services and Open  
Government**

By: \_\_\_\_\_

  
Dave Nikolejsin  
Government Chief Information Officer

Agreed to and accepted this 26<sup>th</sup> day of July, 2012 by the Supplier.

**SecureKey Technologies Inc.**

By:   
Name: Jaime Shapiro  
Title: President

## **EXHIBIT A**

### **BC Services Card Transition Design Specification**

Attached.

Pages 14 through 28 redacted for the following reasons:

-----

s 15



February 1, 2013

HER MAJESTY THE QUEEN IN RIGHT OF THE PROVINCE OF BRITISH COLUMBIA, as represented by the Minister of Labour, Citizens' Services and Open Government (the "Province").

4000 Seymour Place  
Victoria, British Columbia  
V8X 4S8

To the attention of:  
Ministry of Labour, Citizen Services and Open Government, Technical Services Division

SecureKey Technologies Inc. ("SecureKey") hereby provides this Notice of Readiness in accordance with the provisions of Section 2 of Schedule 3.2 of the Master Services Agreement entered into by the Province and SecureKey dated April 13, 2012 (the "MSA"). The criteria of Section 1 of Schedule 3.2 of the MSA have been satisfied and SecureKey has delivered the following Test Components (described in detail in Appendix 2.2 to Schedule 1.5 of the Card Management Services SOW under the MSA) for the purposes of Acceptance Testing:

- (a) *Personalization and authentication using test cards*
- (b) *Personalization and authentication using production cards*
- (c) *Services Card status updates*

We further confirm the readiness of the four key elements of the Card Management Services (i.e., PAN Management and Assignment, Services Card Personalization, Card Management Database, Services Card Status Updates), as described in Section 1 of Appendix 2.2 to Schedule 1.5 of the Card Management Services SOW under the MSA.

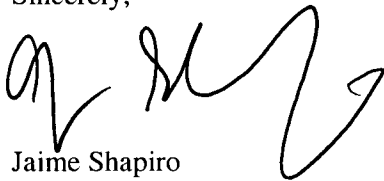
In addition, SecureKey has provided the following items to the Province:

- a) Copies of all reasonable supporting information, including all design documents, test results.
  - i. Previously submitted to the Province:
    - IAS and CMS Interface Design Specification v1.3
    - IRIS and CMS Interface Design Specification v1.0
    - BC Services Card and SecureKey Issuance and Lifecycle Management Business Requirements Overview v1.3
    - SecureKey Service Card High Level Details v1.5
    - CMS Program Wide Security Design v1.9
    - BC Services Card SecureKey Card Management System Test Strategy v0.6
    - SecureKey Chip Management System Export-Import File Format v2.1

- ii. Included in this Notice of Readiness:
  - Email confirmations of IRIS Personalized PAN list files
  - Testing Summary Report listing any outstanding defects
- b) Test environment (including establishing, hosting, supporting and maintaining the test environment) along with physical or remote access by the Province to the test environment;
- c) User acceptance test environment that supports multiple test instances to enable the Province to test its own different identity environments.
- d) Transition File materials for testing as per the Specification document (ref #DOCS-#11613067-v9-Exhibit\_A\_-\_BC\_Services\_Card\_Transition\_Design\_Specification).
  - i. In addition SecureKey provided this supporting document: Decrypt Transition File User Guide v1.2

SecureKey looks forward to receiving the Province's response to this Notice of Readiness by February 8, 2013, the target date discussed by the Joint Operations Committee at its recent meeting.

Sincerely,

A handwritten signature in black ink, appearing to read 'Jaime Shapiro', is written over the printed name.

Jaime Shapiro  
President



<b>Subject</b>	<b>September Shipment [Quantity - 275,000] - Personalized PAN List File</b>
<b>From</b>	<u>Khairul Azwar</u>
<b>To</b>	Chris Chapman; Jason Harley; Eli Erlikhman
<b>Cc</b>	'Yeoh Suat Lay '; bahjat@iris.com.my; 'Nicholas Tan'; Mazrin@iris.com.my; m.nazim@iris.com.my
<b>Sent</b>	Tuesday, September 25, 2012 5:15 AM

Dear Team,

For your information, Personalized PAN List file for September shipment has been uploaded to your server and ready to be processed. There is no End-Of-Life file as there is no damaged Pan for this batch. Following are the list of filenames uploaded –

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.
- 9.
- 10
- 11
- 12
- 13
- 14
- 15

s 15

Total PAN number is 224,500. The remaining of 50,000 will be uploaded after the cards has been shipped out on 5<sup>th</sup> October 2012.

Please acknowledge the receipt and highlight to us if you have any issue related to the file.

Thank you.

Regards,

Khairul Azwar

IRIS Corporation Berhad

IRIS Smart Technology Complex, Technology Park Malaysia, Bukit Jalil, 57000 Kuala Lumpur.

Tel : +603-89960788 ext 1126 | Fax : +603-89960451 | [www.iris.com.my](http://www.iris.com.my)



<b>Subject</b>	<b>September Shipment [Quantity - 275,000] - Personalized PAN List File (Remaining 50000)</b>
<b>From</b>	<u>Khairul Azwar</u>
<b>To</b>	Chris Chapman; Jason Harley; Eli Erlikhman
<b>Cc</b>	'Yeoh Suat Lay '; bahjat@iris.com.my; 'Nicholas Tan'; Mazrin@iris.com.my; m.nazim@iris.com.my
<b>Sent</b>	Monday, October 08, 2012 1:52 AM

Dear Team,

For your information, Personalized PAN List file for the remaining September shipment has been uploaded to your server and ready to be processed. There is no End-Of-Life file as there is no damaged PAN number for this batch. Following are the list of filenames uploaded –

- 1.
2. s 15
- 3.

Total PAN number is 50000.

Please acknowledge the receipt and highlight to us if you have any issue related to the files.

Thank you.

Regards,

Khairul Azwar

IRIS Corporation Berhad

IRIS Smart Technology Complex, Technology Park Malaysia, Bukit Jalil, 57000 Kuala Lumpur.

Tel : +603-89960788 ext 1126 | Fax : +603-89960451 | [www.iris.com.my](http://www.iris.com.my)

**IRIS**<sup>®</sup>  
Bringing Solutions to Life

<b>Subject</b>	<b>October Shipment [Quantity - 230,000] - Personalized PAN List File</b>
<b>From</b>	<u>Khairul Azwar</u>
<b>To</b>	Chris Chapman; Jason Harley; Eli Erlikhman
<b>Cc</b>	'Yeoh Suat Lay '; bahjat@iris.com.my; 'Nicholas Tan'; Mazrin@iris.com.my; m.nazim@iris.com.my
<b>Sent</b>	Thursday, October 25, 2012 7:34 AM

Dear Team,

For your information, Personalized PAN List file for October shipment has been uploaded to your server and ready to be processed. There is no End-Of-Life file as there is no damaged Pan for this batch. Following are the list of filenames uploaded –

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.
- 9.

s 15

Total PAN number is 230,000.

Please acknowledge the receipt and highlight to us if you have any issue related to the file.

Thank you.

Regards,

Khairul Azwar

IRIS Corporation Berhad

IRIS Smart Technology Complex, Technology Park Malaysia, Bukit Jalil, 57000 Kuala Lumpur.

Tel : +603-89960788 ext 1126 | Fax : +603-89960451 | [www.iris.com.my](http://www.iris.com.my)

**IRIS**<sup>®</sup>  
Bringing Solutions to Life

<b>Subject</b>	<b>January Shipment [Quantity - 320,000] - Personalized PAN List Files</b>
<b>From</b>	<u>Khairul Azwar</u>
<b>To</b>	Chris Chapman; Jason Harley; Eli Erlikhman
<b>Cc</b>	'Yeoh Suat Lay '; bahjat@iris.com.my; 'Nicholas Tan'; Mazrin@iris.com.my; m.nazim@iris.com.my
<b>Sent</b>	Wednesday, January 16, 2013 4:35 AM

Dear Team,

For your information, Personalized PAN List files for January shipment have been uploaded to your server and ready to be processed. There is no End-Of-Life file as there is no damage PAN for this batch. Following are the list of filenames uploaded –

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.
- 9.

s 15

Total PAN number is 320,000.

Please acknowledge the receipt and highlight to us if you have any issue related to the file.

Thank you.

Regards,

Khairul Azwar

IRIS Corporation Berhad

IRIS Smart Technology Complex, Technology Park Malaysia, Bukit Jalil, 57000 Kuala Lumpur.

Tel : +603-89960788 ext 1126 | Fax : +603-89960451 | [www.iris.com.my](http://www.iris.com.my)

**IRIS**<sup>®</sup>  
Bringing Solutions to Life

s 15

s 15

s 15

s 15



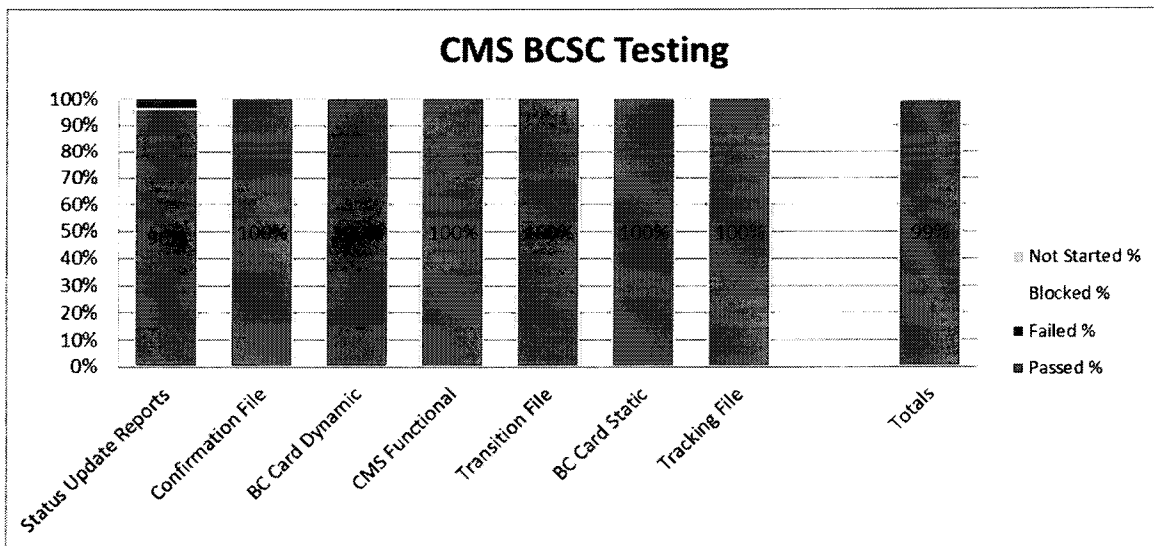
s 15

## CMS Outstanding Items

No.	Item	Status
1.	Transition File Testing: Script and DB reconciliation	CITZ testing in progress
2.	Confirmation file Signature Value	Fixed delivered to CITZ Jan 31. To be validated.
3.	REPORT_UPDATES report not working for daily option. Weekly option validated.	Ticket raised with BellID Feb 1, 2013. Fix pending delivery to SecureKey.

## CMS Test Summary Report

Test Plan	Total Planned	Passed	Passed %	Failed	Failed %	Blocked	Blocked %	Not Started	Not Started %	Percent Executed
Status Update Reports	26	25	96%	1	4%	0	0%	0	0%	100.0%
Confirmation File	19	19	100%	0	0%	0	0%	0	0%	100.0%
BC Card Dynamic	20	20	100%	0	0%	0	0%	0	0%	100.0%
CMS Functional	62	62	100%	0	0%	0	0%	0	0%	100.0%
Transition File	2	2	100%	0	0%	0	0%	0	0%	100.0%
BC Card Static	16	16	100%	0	0%	0	0%	0	0%	100.0%
Tracking File	3	3	100%	0	0%	0	0%	0	0%	100.0%
<b>Totals</b>	<b>148</b>	<b>147</b>	<b>99%</b>	<b>1</b>	<b>1%</b>	<b>0</b>	<b>0%</b>	<b>0</b>	<b>0%</b>	<b>100.0%</b>





Ref: 97787

February 8, 2013

Mr. Jaime Shapiro  
President  
SecureKey Technologies Inc.  
Suite 2900, 199 Bay St.  
PO Box 366  
Toronto, Ontario  
M5L 1G2

Dear Jaime Shapiro:

**Re: SecureKey Notice of Readiness Feb 01 2013**

Subject to the conditions and qualifications below, the Province hereby provides this Notice of Acceptance for Test Components, in accordance with the provisions of Section 6 of Schedule 3.2 of the Master Services Agreement entered into by the Province and SecureKey Technologies Inc. ("SecureKey"), dated as of April 13, 2012 (the "MSA"). The Province hereby accepts the following Test Components for purposes of Schedule 3.2 of the MSA:

1. The following Test Components described in detail in Appendix 2.2 to Schedule 1.5 of the Card Management Services SOW under the MSA:
  - (i) Personalization and authentication using test cards
  - (ii) Personalization and authentication using production cards
  - (iii) Services Card Status updates
2. The four key elements of the Card Management Services (i.e. PAN Management and Assignment, Services Card Personalization, Card Management Database, Services Card Status Updates), as described in Section 1 of Appendix 2.2 to Schedule 1.5 of the Card Management Services under the MSA

subject to the following conditions and qualifications:

- The Province has not yet completed testing the following CMS Operational Reports, which were delivered after the SecureKey "Notice of Readiness" letter:
  - Card Management Processing Time
  - Monthly Time to Restore Summary
  - Monthly Tier 3 Support Summary
  - P1 P2 Time to Restore
  - P3 P4 Time to Restore

The Province expects to complete testing on these reports, and respond to SecureKey with an Acceptance or Failure Notice, by February 22, 2013. Accordingly, these reports have not yet been accepted by the Province for purposes of Schedule 3.2 of the MSA.

- A defect has been identified in how CMS handles card status reports related to error situations (Issue #7366 – “Sometimes CMS generates Zero byte card status updates Reports”). Accordingly, the Province does not accept the Test Component that has this defect, and this letter will be deemed to be a Failure Notice with respect to such Test Component. SecureKey must address by March 31, 2013, then notify the Province so a re-test can be performed.
- The Province will perform additional Transition File testing with SecureKey, and request updated versions of the *BC Services Card Transition Design Specifications* and *Decrypt Transition File User Guide* documents, to be completed before March 31, 2013. Accordingly, these documents have not yet been accepted by the Province for purposes of Schedule 3.2 of the MSA.

The Province looks forward to receiving the Notice of Readiness for Card Management Services in Production from SecureKey by February 11<sup>th</sup>, the target date discussed by the Joint Operations Committee at its meeting on January 25<sup>th</sup>, 2013.

Sincerely,



Kevena Bamford  
Executive Director  
Provincial IDIM Program

pc: Andre Boysen, SecureKey Technologies Inc.  
Heather Neale, SecureKey Technologies Inc.  
Chris Chapman, SecureKey Technologies Inc.  
Ian Bailey, Ministry of Citizens' Services and Open Government  
Patricia Wiebe, Ministry of Citizens' Services and Open Government  
Jeremy Moss, Ministry of Citizens' Services and Open Government



February 11, 2013

HER MAJESTY THE QUEEN IN RIGHT OF THE PROVINCE OF BRITISH COLUMBIA, as represented by the Minister of Citizens' Services and Open Government (the "Province").

4000 Seymour Place  
Victoria, British Columbia  
V8X 4S8

To the attention of:  
Ministry of Citizen Services and Open Government

SecureKey Technologies Inc. ("SecureKey") is pleased to provide this Notice of Readiness for Production. We confirm the production readiness of the four key elements of the Card Management Services (i.e., PAN Management and Assignment, Services Card Personalization, Card Management Database, Services Card Status Updates), as described in Section 1 of Appendix 2.2 to Schedule 1.5 of the Card Management Services SOW under the Master Services Agreement entered into by the Province and SecureKey dated April 13, 2012.

In addition, SecureKey is providing the following items to the Province:

- a) Copies of all reasonable supporting information, including all design documents, test results, escrow material deposit confirmation and PCI DSS attestation.
- b) Service Management agreement has been drafted and processes/procedures are in place to support Production.
- c) CMS Operational Reporting Design drafted and Test Reports provided to CITZ as designed.
- d) CMS traceability matrix update. CMSLCM-19 PAN re-use fully tested and confirmed meets requirements as designed.

SecureKey looks forward to receiving the Province's response to this Notice of Readiness by February 21, 2013, the target date discussed by the Joint Operations Committee at its recent meeting.

Sincerely,

A handwritten signature in black ink, appearing to read "Jaime Shapiro".

Jaime Shapiro  
President

Copy of Iron Mountain Escrow submission

Canadian Vault/Reference s 15

EXHIBIT B

## DEPOSIT MATERIAL DESCRIPTION

Deposit Account Number: s 15

COMPANY NAME: SECUREKEY TECHNOLOGIES INC.

DEPOSIT NAME s 15

s 15

DEPOSIT MEDIA (PLEASE LABEL ALL MEDIA WITH THE DEPOSIT NAME PROVIDED ABOVE)

MEDIA TYPE	QUANTITY	MEDIA TYPE	QUANTITY
<input type="checkbox"/> Internet File Transfer	N/A	<input type="checkbox"/> 3.5" Floppy Disk	
<input type="checkbox"/> CD-ROM / DVD		<input type="checkbox"/> Documentation	
<input type="checkbox"/> DLT Tape		<input type="checkbox"/> Hard Drive / CPU	
<input type="checkbox"/> DAT Tape		<input type="checkbox"/> Circuit Board	

☒ Other (describe here):

Tamper Evident Envelopes Labeled With The Applicable Deposit Name Provided Above

DEPOSIT ENCRYPTION (Please check either "Yes" or "No" below and complete as appropriate)

Is the media or are any of the files encrypted? ☐ Yes or ☒ No

If yes, please include any passwords and decryption tools description below. Please also deposit all necessary encryption software with this deposit.

Encryption tool name \_\_\_\_\_ Version \_\_\_\_\_

Hardware required \_\_\_\_\_

Software required \_\_\_\_\_

Other required information \_\_\_\_\_

DEPOSIT CERTIFICATION (Please check the box below to Certify and Provide your Contact Information)

<input checked="" type="checkbox"/> I certify for Depositor that the above described Deposit Material has been transmitted electronically or sent via commercial express mail carrier to Iron Mountain at the address below.	<input type="checkbox"/> Iron Mountain has inspected and accepted the above described Deposit Material either electronically or physically. Iron Mountain will notify Depositor of any discrepancies.
NAME: JAIME SHAPIRO	NAME:
DATE: FEBRUARY 11, 2013	DATE:
EMAIL ADDRESS: JAIME.SHAPIRO@SECUREKEY.COM	
TELEPHONE NUMBER: 416-477-5621	
FAX NUMBER: 416-221-7249	

**Note: If Depositor is physically sending Deposit Material to Iron Mountain, please label all media and mail all Deposit Material with the appropriate Exhibit B via commercial express carrier to the following address:**

Mr. Ralph Mackinnon  
 Iron Mountain Off-Site Data Protection  
 Reference #72943  
 195 Summerlea Road  
 Brampton, ON L6T 4P9  
 Canada

Email copy to:  
 IPMVaultAdministrators@ironmountain.com

## Excerpt PCI DSS Attestation

**Part 3a. Confirmation of Compliant Status****Service Provider confirms:**

- ☒ Self-Assessment Questionnaire D, Version 2, was completed according to the instructions therein.
- ☒ All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment.
- ☒ I have read the PCI DSS and I recognize that I must maintain full PCI DSS compliance at all times.
- ☒

s 15

**Part 3b. Service Provider Acknowledgement**

March 13, 2012

Signature of Service Provider Executive Officer ↑

Date ↑

Dmitry Barinov

Chief Security Officer

Service Provider Executive Officer Name ↑

Title ↑

SecureKey Technologies Inc.

Service Provider Company Represented ↑

**Part 4. Action Plan for Non-Compliant Status**

Please select the appropriate "Compliance Status" for each requirement. If you answer "NO" to any of the requirements, you are required to provide the date Company will be compliant with the requirement and a brief description of the actions being taken to meet the requirement. *Check with your acquirer or the payment brand(s) before completing Part 4, since not all payment brands require this section.*

<sup>5</sup> Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorization. The only elements of track data that may be retained are account number, expiration date, and name.

<sup>6</sup> The three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card-not-present transactions.

<sup>7</sup> Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.



Oct 15, 2013.

HER MAJESTY THE QUEEN IN RIGHT OF THE PROVINCE OF BRITISH COLUMBIA, as represented by the Ministry of Technology, Innovation and Citizens' Services  
Government (the "Province").  
4000 Seymour Place  
Victoria, British Columbia  
V8X 4S8

To the attention of:  
Ministry of Technology, Innovation and Citizens' Services

SecureKey Technologies Inc. ("SecureKey") hereby provides this Notice of Readiness in connection with certain Test Components of the Authentication Services in accordance with the provisions of Section 2 of Schedule 3.2 of the Master Services Agreement entered into by the Province and SecureKey dated April 13, 2012 (the "MSA"). The criteria of Section 1 of Schedule 3.2 of the MSA have been satisfied with respect to the Test Components below (described in detail in Appendix 2.3 to Schedule 1.5 of the Authentication Services SOW under the MSA) and such Test Components are ready for review and testing by the Province:

- a. Authentication with USB terminal*
- b. User Interface*
- c. Reporting*
- d. Security*

We further confirm the readiness of the key elements of the Authentication Services, as described in Appendix 2.3 to Schedule 1.5 of the Authentication Services SOW under the MSA.

1. EMV Cryptographic Authentication. Where a Services Card is presented to a Terminal, Supplier will:
  - a) verify whether (A) the EMV cryptogram produced by the Services Card is valid (B) the Services Card is active
  - b) where a Services Card is not valid, not active or both, (a "Fail Result") Supplier will fail authentication
  - c) if the Services Card is both valid and active, a "Pass Result"



2. User Interface. Supplier will use best efforts to ensure that all user interface for the Authentication Service comply with requirements set out in the SOW.
3. Security Specifications. Supplier's authentication system is resistant to security threats using industry standard security testing tools.

Other Items:

1. USB Terminals:
  - a. USB Authentication Tokens and prototype USB Counter Devices are available for testing.
2. Documentation:
  - a) Authentication Protocols. The Supplier Authentication Services will integrate with the Province using the JSON protocol and data formats. The Supplier will provide a technical specification document to the Province that describes the JSON profile.
    - SKAP\_BC\_Integration\_Design\_Spec\_v3.11.doc
  - b) SK Security documentation has been made available
    - Various documents have been provided to MTICS
3. Documents included in this Notice of Readiness:
  - c) Card Authentication Test Plan v0.3
  - d) BC Regression Test Exit Report v0.2

In addition, SecureKey has provided the following items to the Province:


- a) User acceptance test environment that supports multiple test instances to enable the Province to test its own different identity environments.
- b) Additional CMS test environment

Outstanding items:

1. Reporting.
  - a. Reporting design is in draft. Completion pending design review sessions.
2. Performance Testing results to be available November 25, 2013.

SecureKey looks forward to receiving the Province's response to this Notice of Readiness by October 21, 2013.

Sincerely,



Jaime Shapiro  
President



# **CARD AUTHENTICATION PERFORMANCE TEST PLAN**

**V0.3**

This document is the property of SecureKey Technologies Inc. (SecureKey). All information contained in this document is confidential and proprietary to SecureKey.

Please note that any disclosure, distribution, or copying of this document or the information in it is regulated by a confidentiality agreement with SecureKey. The document and information may not be copied, distributed or recorded in any electronic, physical, or other medium without the prior express written permission of SecureKey or otherwise in accordance with the confidentiality agreement.

**Revision:** 0.3

**Effective Date:** 1 August 2013

**Owner:** Navin Shenoy

**Approver:** Chris Chapman

CLASSIFICATION | **SECUREKEY SENSITIVE | PROTECTED A**

## Document Control Change Record

Date	Revision	Section(s)	Editor	Change Reference
16/08/2013	0.1	All	Navin Shenoy	Initial Draft
26/08/2013	0.2	All	Navin Shenoy	Updated based on BC comments. Added Benchmarking process details, Details on how caching will be handled
	0.3	All	Navin Shenoy	Updated based on BC comments

Document Reference: V0.3  
Revision: 0.3  
Effective Date: 080113

Classification: **SENSITIVE**

Page 2 of 11

## Stakeholders / Contributors

Department	Stakeholder / Contributor	Role

Document Reference: V0.3  
Revision: 0.3  
Effective Date: 080113

Classification: **SENSITIVE**

Page 3 of 11

## Table of Contents

1. Introduction .....	5
1.1 Purpose .....	5
2. Performance Testing Strategy .....	6
2.1 Performance Objectives .....	6
2.2 Scope .....	6
2.3 Approach .....	7
2.4 Performance Measurement transaction scope .....	9
3. Load Testing Results .....	11

Document Reference: V0.3  
Revision: 0.3  
Effective Date: 080113

Classification: **SENSITIVE**

Page 4 of 11

# 1. Introduction

## 1.1 Purpose

This document serves as Performance Test plan for the Card Authentication API of briidge.net Platform (Access Platform). The Performance Test Plan is intended to demonstrate that the performance requirements of the briidge.net system, as defined by the BC Statement of Work (SOW) are met.

The Performance Test plan covers the following:

- High-level approach, including defining criteria of performance testing and methods of performance metrics measurement
- Testing harness implemented using Java and enhanced Jmeter functionality
- Test Cases defining the tasks that need to be executed
- Test results which meet or exceed performance objectives as defined in the SoW

Additionally Benchmarking of the briidge.net widget will be carried.

## 2. Performance Testing Strategy

### 2.1 Performance Objectives

As defined in the SoW, the following performance objectives must be demonstrated:

- Authentication request complete in 2 secs 95% of time. Scope of authentication request for measurement purpose has been defined in the "Performance Measurement Transaction scope" section of the document.
- Sustained Load of 10 simultaneous authentication attempts per sec for 1 hour
- 100 test card numbers to avoid caching of data

#### Benchmarking objectives

Benchmarking will be carried out for widget by recording time between SKAP.init call and onConnected and SKAP.init call and when the card tap prompt is shown to the user.

### 2.2 Scope

s 15

Classification: **SENSITIVE**

Document Reference: V0.3  
Revision: 0.3  
Effective Date: 080113

Page 6 of 11



- Bridge.net (SecureKey Access Platform) card based authentication API
- Card Verification Service (CVS)
- Card Management Service (CMS)

The following items are out of scope for performance testing

- SK USB Token/Cards (Data will be simulated using JMeter)
- Any non SK components (e.g. BC Systems)
- § 15 API for cryptogram Verification
  - Only sanity load test will be carried out on § 15 api by applying load upto 2 transaction per sec if the § 15 test environment supports it.
  - For the SK Performance testing report the performance testing results provided by § 15 will be manually added to the performance of SK components to provide a more accurate picture of expected system performance.

## Environment

### 2.3 Approach

#### 2.3.1 Authentication Performance testing

1>

2>

§ 15

3>

4> The following important results will be published.

---

Document Reference: V0.3  
Revision: 0.3  
Effective Date: 080113

Classification: **SENSITIVE**

Page 7 of 11

- Test criteria used to generate the report (ramp up time , duration for test, no of simultaneous requests)
- Avg Card Authentication time
- Min Card Authentication time
- Max Card Authentication time
- Response Time graph by averaging responses every 5 min

### 2.3.2 Widget Benchmarking

- 1> JUnit test cases using Firefox Selenium tools will be used to Benchmark widget running it continuously for 1 hr. Benchmarking should be carried out on the while the environment is undergoing performance tests and a token physical connected to the USB on the machine where benchmarking is being carried out.
- 2> The JUnit test cases will record time between
  - a. SKAP.init and onConnected event
  - b. SKAP.init and tap card graphics display event
- 3> The following important results will be published.
  - Test criteria used to generate the report (ramp up time , duration for test, no of simultaneous requests)
  - Avg , min and max times for each of the previously recorded times.
  - Response Time graph by averaging responses every 5 min

## 2.4 Test Case

### 2.4.1 Briidge.net

The test case selected are on the basis of the longest possible execution path in Briidge.net Authentication API Call including Card Verification service. s 15 Cryptogram Verification will be excluded by setting card status to Personalized. This should allow measured data to be a true indicator of Card Verification Service and briidge.net performance. s 15 Verification Performance results published by s 15 will be added to the performance measured from Briidge.net

#### Test Pre steps

- 1>
- 2> s 15

#### Test Steps

- 1>
- 2> s 15
- 3> .

Document Reference: V0.3  
Revision: 0.3  
Effective Date: 080113

Classification: **SENSITIVE**

Page 8 of 11

- 4> Repeat test case for specified load  
Ramp up to specified load in 15 and run the tests at sustained specified load continuously for 1 hr.  
Ensure cards are picked from a database of 100 cards to avoid caching.
- 5> Extract test response from briidge.net event log database.

## 2.5 Performance Measurement transaction scope

The figure below describes the authentication processing time measurement boundaries. SecureKey performs event logging on selected events. The relevant events for this measurement are:

1. Receipt of GetAuthData response from card authentication
2. AP response for user interaction request is ready for RP data retrieval

For Performance measurement, only the times from the start and end marked in the sequence diagram will be measured and reported

Card Authentication Sequence Diagram

s 15

Classification: **SENSITIVE**

Document Reference: V0.3  
Revision: 0.3  
Effective Date: 080113

Page 10 of 11

## 2.6 Performance Testing Schedule

Task	Responsible party	Date
Environment Setup	SK Ops	Upto Nov 11
Execute Performance tests	SK Ops	Nov 11
Carry out hardware and software optimization if required	SK Dev/SK PS/SK Ops	Nov 18
Publish Results	SK PS	Nov 25

## 3. Load Testing Results

To be completed after completion of load testing.



## TEST EXIT REPORT

### BC REGRESSION TESTING

This document is the property of SecureKey Technologies Inc. (SecureKey). All information contained in this document is confidential and proprietary to SecureKey.

Please note that any disclosure, distribution, or copying of this document or the information in it is regulated by a confidentiality agreement with SecureKey. The document and information may not be copied, distributed or recorded in any electronic, physical, or other medium without the prior express written permission of SecureKey or otherwise in accordance with the confidentiality agreement.

**Revision:** 0.2

**Effective Date:** 16 August 2013

**Owner:** Ayinde Yakubu/Navin Shenoy

**Approver:** Chris Chapman

CLASSIFICATION | **SECUREKEY SENSITIVE | PROTECTED A**

<b>Product</b>	BC Services Card Program	<b>Build</b>	CMS: 6.4.3.13.2 AP 2.1 Token SW version: 2.1.0.6715
<b>Environment</b>	QA	<b>Test iterations</b>	3
<b>Start Date</b>	Jul. 2 <sup>th</sup> , 2013	<b>End Date</b>	Aug. 16 <sup>th</sup> , 2013
<b>Test Plans</b>	Bridge.net Enterprise 2.0 testing plans		
<b>Status</b>	<b>Passed</b>	<b>Date</b>	Aug. 22th, 2013

# 1. Introduction

## 1.1 Test Scope

The bridge.net Enterprise™ and Card Management System are part of the overall solution design for the BC Services Card Program.

Baseline testing was based on:

- SKAP\_BC\_Integration\_Design\_Spec\_v3.11.docx
- Credential Authentication Design\_v1.7.docx
- BCSC\_IAS\_CMS\_Interface\_Design\_Specification\_v1\_4.docx

The following functions were fully tested:

1. Bridge.net authentication service
2. Card Verification service and all the authentication error codes documented in Integration design document
3. Card Lifecycle –Card Status
4. PANs State transition
5. MBUN State transition
6. File processing of End-Of-Life file PAN, End-Of-Life MBUN, personalized pan list file, PAN activate list file
7. Confirmation of Card Status Updates Report
8. Report of Card Status Updates

Document Reference: BC REGRESSION TESTING

Revision: 0.2

Effective Date: 16 August 2013

CLASSIFICATION | **SECUREKEY SENSITIVE** | **PROTECTED A**

Page 2 of 7

Scope of this testing will include the following OS and browsers:

OS	Browser	Supported Versions
<b>Microsoft Windows XP</b>	IE	IE 8
	Firefox	Current release plus 2 versions back
	Chrome	Current release plus 1 versions back
<b>Microsoft Windows Vista</b>	IE	IE 8,9
	Firefox	Current release plus 2 versions back
	Chrome	Current release plus 1 versions back
<b>Microsoft Windows 7</b>	IE	IE 8,9,10
	Firefox	Current release plus 2 versions back
	Chrome	Current release plus 1 versions back
<b>Windows 8</b>	IE	IE 10
	Firefox	Current release plus 2 versions back
	Chrome	Current release plus 1 versions back
<b>Apple Mac OS X</b>	Safari	Current release plus 1 versions back
	Firefox	Current release plus 2 versions back
	Chrome	Current release plus 1 versions back

Following functions were excluded from the exit report

- Integration testing with BC
- Performance testing of Bridge.net authentication service

## 2. Test Results

Document Reference: BC REGRESSION TESTING

Revision: 0.2

Effective Date: 16 August 2013

CLASSIFICATION | **SECUREKEY SENSITIVE | PROTECTED A**

Page 3 of 7



# TEST EXIT REPORT

As shown in the table below, all planned tests were successfully executed. All the test passed at 100%.

Test Plan	Number of Test Cases					Execution Percentages				
	Total Planned	Passed	Failed	Blocked	Not Started	Passed %	Failed %	Blocked %	Not Started %	Percent Executed
Mac OS X	48	48	0	0	0	100%	0%	0%	0%	100%
BC Card - Dynamic	20	20	0	0	0	100%	0%	0%	0%	100%
BC Card - Static	16	16	0	0	0	100%	0%	0%	0%	100%
Windows OS	48	48	0	0	0	100%	0%	0%	0%	100%
Counter Reader	70	70	0	0	0	100%	0%	0%	0%	100%
<b>Totals</b>	<b>202</b>	<b>202</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>100%</b>	<b>0%</b>	<b>0%</b>	<b>0%</b>	<b>100%</b>

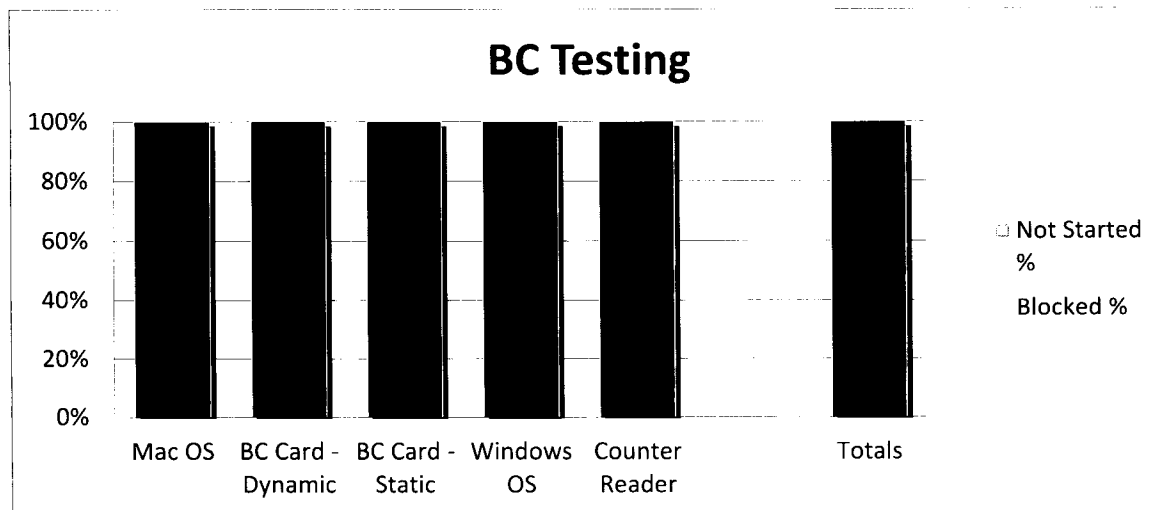


Figure 1. Test Execution Percentage Diagram

All planned tests were executed with none blocked.

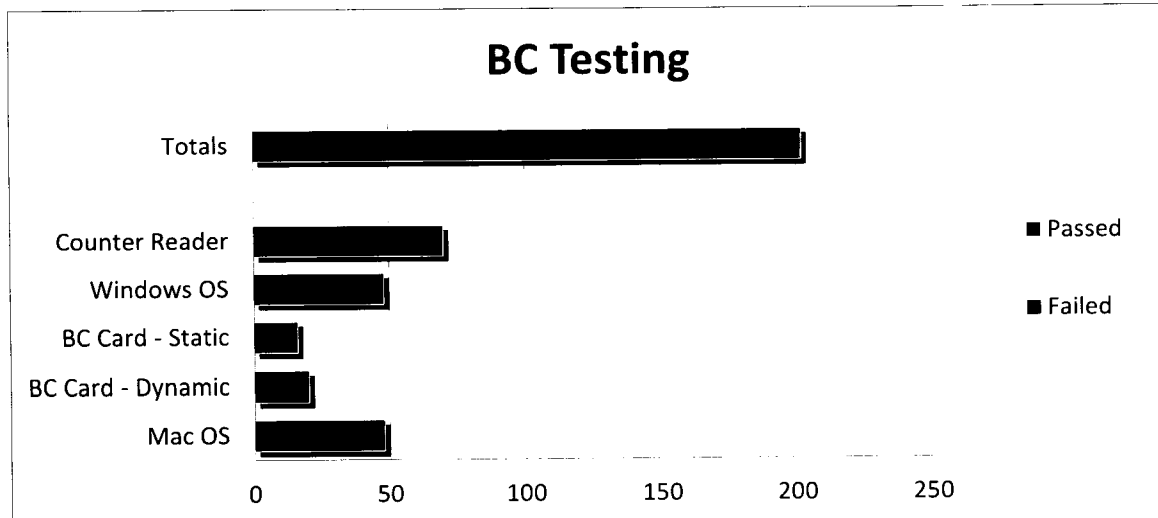


Figure 2. Test Success Percentage Diagram

In testing the existing functionalities of the system, 2 categories of tests were carried out: static and dynamic card tests. In the case of static tests, the card is assumed to be at a state of rest. SecureKey uses our test console tool to simulate card authentication initiation requests and responses. In the case of dynamic tests, validation is done on an integrated Card Management System (CMS) in conjunction with authentication flows.

The following static tests were conducted:

- Testing the status of a card created with and without an MBUN
- Testing the status of a card personalized with and without an MBUN
- Testing the status of a card activated with and without an MBUN
- Testing the status of a card that is in use with and without an MBUN
- etc

The following dynamic tests were conducted:

Changing card status according to the state transition in the CMS Interface design documents. Although all the state transitions were tested only a few of the state transitions tested are listed below

- Changing the status of card from created to personalized
- Changing the status of card from created to deactivated when the card is damaged
- Changing the status of card from personalized to activated
- Changing the status of card from on hold to inuse
- etc

We also conducted authentication tests. These include:

- Failed reading of a card via the counter terminal using test cards which return failed card read.
- Initial setup of the terminal
- Verification of whether the terminal is in the ready to use state
- Successful reading of a card via the counter terminal

Document Reference: BC REGRESSION TESTING

Revision: 0.2

Effective Date: 16 August 2013

CLASSIFICATION | **SECUREKEY SENSITIVE** | **PROTECTED A**

Page 5 of 7

- Card authentication process - this exercises briidge.net enterprise server as well
- Reading of card when no token is plugged in
- etc

Each of these tests were successfully run and passed.

### 3. Defect Summary

s 15

## 4. Recommendation

QA recommends proceeding to User Acceptance Testing and BC Integration testing.

Document Reference: BC REGRESSION TESTING

Revision: 0.2

Effective Date: 16 August 2013

CLASSIFICATION | **SECUREKEY SENSITIVE | PROTECTED A**

Page 7 of 7