Provincial IDIM Program
BC Services Card Project

Identity Assurance Services
Solution Architecture Overview

Version: 1.0
2016-12-22

Document Information

Document title	IAS Solution Architecture Overview
Revision number	1.0
Issued by	Patricia Wiebe, Director of Identity Architecture Provincial Identity Information Management Program
Issue Date	2016-12-22

Document Purpose and Intended Audience

This document provides an introduction and overview of the solution architecture of the Identity Assurance Services (IAS), the foundational system that manages identity and card lifecycle information and provides identity information and authentication services for the BC Services Card program.

Document Contents

Figures

Tables

1. EXECUTIVE SUMMARY

The **BC Services Card** is a type of government-issued identification that started to be issued by the Province of BC to its residents in February 2013. The card is a replacement for the Ministry of Health's Care Card, and also intended as a convenient card that can be used to access many other government services.

The card is both a physical identity credential and a smartcard that can be electronically authenticated. The BC Services Card offers a digital equivalent of a driver licence that an **individual can use to prove their identity to access to online services**.

The BC Services Card Program is an integrated program between the Ministry of Health (Health), the Insurance Corporation of British Columbia (ICBC) and the Ministry of Technology, Innovation and Citizens' Services (MTICS).

MTICS has developed the **Identity Assurance Services** (IAS) as their foundational system to provide provincial identity information services that:

- manage registered identity information of BC residents who are issued cards;
- authenticate the card when a person chooses to use it; and,
- provide identity information to government services.

Government services are delivered in different ways (in person, online, through mail or telephone) and use different methods to identify an individual. Some government services require a high degree of confidence (identity assurance) about the individual they are serving before providing access or information.

The BC Services Card provides **increased identity assurance** and **consistency of identification and identity information** to government programs and services, and is intended to make it **more convenient and secure** for cardholders to access services. The card and its services are envisioned to be a significant **enabler in delivering online government services**.

This document provides an overview of the solution architecture of the Identity Assurance Services, including:

- the overall business context of the BC Services Card program and the Provincial Identity Information Management Program;
- the key business scenarios of card issuance, online authentication, passcode issuance, account management, onboarding and support; and,
- an overview of its application, data, technology and security architecture.

2. INTRODUCTION

2.1. BC Services Card

The BC Services Card is a type of government-issued identification issued by the Province of British Columbia, as a replacement for the Ministry of Health's Care Card. The card is a physical credential that can be used to prove a set of facts about an individual, such as name and date of birth. The card is also a smartcard credential that is capable of being electronically authenticated. The card is backed by provincial identity information services that manage registered identity information, authenticate the card when a person uses it, and provide identity information to government services.

Government services are delivered in different ways (in person, online, through mail or telephone) and use different methods to identify an individual. Some government services require a high degree of confidence (identity assurance) about the individual they are serving before providing access or information.

The BC Services Card provides increased identity assurance and consistency of identification to government programs and services, and is intended to make it more convenient and secure for cardholders to access services. The card and its services are envisioned to be a significant enabler in delivering online government services.

2.1.1. Card Types

There are three types of BC Services Cards:

1. Combination Driver's licence and BC Services Card ("Combo")
An individual may elect to combine these two cards for convenience.

2. BC Services Card with a photo ("Standalone")
An individual may elect to have their BC Services Card separate from their driver's licence.

3. BC Services Card without a photo ("Non-photo")
For individuals under 19, or those over 19 with certain exemptions and exceptions.

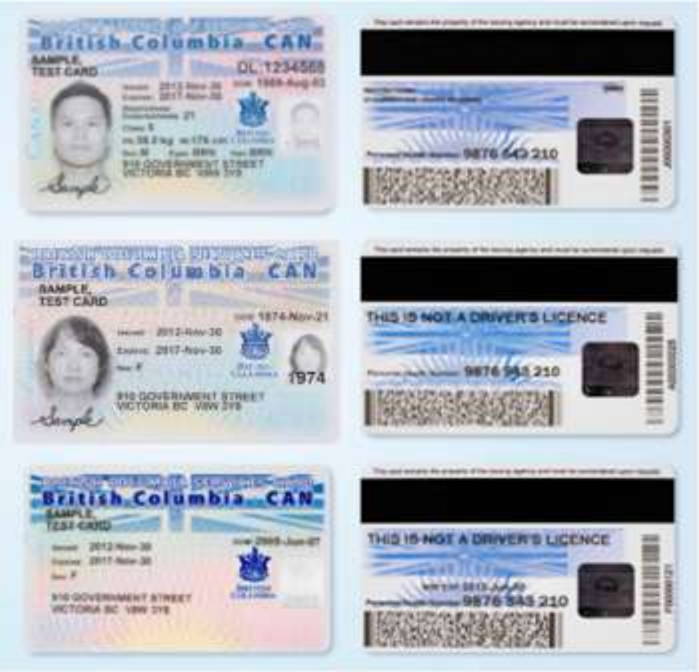


Figure 1: BC Services Card Types

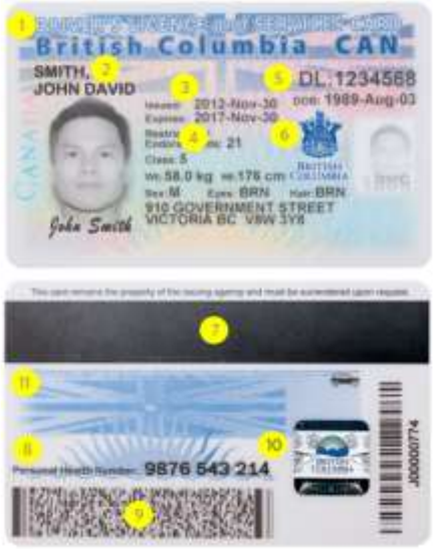
2.1.2. Card Features

All three types of BC Services Card have these features:

- Name, date of birth, sex and address printed on the front side of the card;
- Card issue and expiry dates printed on the front side of the card;
- Personal Health Number (PHN) printed on the back side of the card;
- A magnetic stripe and 2D barcode on the back side of the card; each contains the same personal information as is printed on the card;
- A contactless security chip embedded in the card that contains a unique account number and security keys; it does not contain the personal information that is printed on the card; and,
- A unique serial number is printed on the back side of the card.

The Combo and Standalone card also have a photo and signature printed on the front side of the card. The Combo card also has driver's licence data printed on the front side of the card, just like a regular driver's licence card.

The following illustration shows an example of a Combo BC Services Card.



1. Card Type
2. Full Name
3. Card Issued Date
4. Card Expiry Date
5. Driver's Licence Number
6. Date of Birth

7. Magnetic Stripe
8. Personal Health Number
9. 2D Barcode
10. Chip (not visible)
11. Driver Restrictions

Also, not marked: 1D Barcode with Serial Number on back right side

Figure 2: BC Services Card Features

From a privacy and security perspective, every card has specialized security features that make it extremely difficult both physically and electronically to alter the card or make a counterfeit card. The BC Services Card has all of the same physical security features of a BC driver's licence including, but not limited to:

- Complex high resolution artwork, images and holograms;
- Printing by laser engraving into the layers of the polycarbonate card material;

- Serialized and controlled inventory of blank cards; and,
- Specialized photo imaging.

Electronically, the BC Services Card contains a contactless security chip following the Europay, MasterCard and Visa (EMV) global standard for authenticating card transactions. It is the same type and has the same security features of a contactless chip of a MasterCard or Visa credit card including, but not limited to:

- The chip is programmed with a unique account number;
- The chip is locked to prevent changes after it is manufactured, and is designed to be damaged if it is tampered with; and,
- The chip contains internal cryptographic keys that are used to prove the chip is genuine; these keys are extremely difficult to duplicate and are not accessible by a card reader.

The security chip does not contain any personal information. This means that if a chip is read by an unauthorized card reader or a Near Field Communications (NFC) reader, there is no personal information to be found. This is different from many smartcard implementations in the world where personal information is stored on the chip.

The BC Services Card security chip is a different type than the RFID chip used in the BC enhanced driver’s licence. The RFID chip is used by Canada Border Service Agency to look up your personal information as you wait in line to cross the border into the United States; it works over a distance of up to 30 metres. The BC Services Card security chip requires close proximity (approximately 2 centimetres) to a card reader and is readable using NFC (Near Field Communications) technology.

2.1.3. Card Authentication

When a BC Services Card is used as evidence that an individual is who they say they are, it is called authentication. Authentication is process of determining whether someone or something is, in fact, who or what it is claimed to be. Authentication processes are classified by how many independent “factors” are required to prove the facts; these factors are usually described as “something you have”, “something you know”, and “something you are”.

- “Something you have” is a physical object that you must possess in order to complete the authentication process. A classic example is a key to unlock a door for your house or your car.
- “Something you know” is a fact that only you should know. Common facts used for authentication are account numbers, user IDs and passwords, and credit card and bank card numbers and PINs.
- “Something you are” is a measurement of some property of your body. Fingerprints and facial photographs are common examples of this type of factor.

The combination of factors results in:

- “Single-factor” authentication: only one of the three types of factors is required; e.g., a user ID and password.
- “Two-factor” authentication: two of the three types of factors are required; e.g., a bank card and a PIN; a driver’s licence with a facial match to the photo on the licence.
- “Three-factor”: all three of the types of factor are required; e.g., a key, a passcode, and a fingerprint are all required.

Many government services need to know who an individual is to some degree of confidence, depending on what services they provide and the sensitivity of the information involved. When a government service is first designed or undergoes a major change, it is required to do an identity-related risk assessment to consider the security measures needed to protect information and a privacy impact assessment to confirm the authority to collect, use and disclose personal information. All government programs must follow the *Freedom of Information and Protection of Privacy (FOIPP) Act* and government information security policies and standards to protect citizens’ personal information.

Some government services have minimal requirements for identity assurance, such as when using public transportation, and may not require any proof of identity. Many government services, however, need higher levels of identity assurance. Higher levels require stronger identification and authentication processes to ensure that the individual is entitled to, and receives, the appropriate service from government.

The BC Services Card can be used to achieve identity assurance through single-factor and two-factor authentication. When the chip is used with a card reader it proves that a card is present and valid.

- The card can be used as “something you have” for single-factor authentication to in-person and online services, however this is not recommended for most uses.
- The card can be used as “something you have” with a passcode as “something you know” for two-factor authentication to online services.
- The card can be used as “something you have” with the photo on the card as “something you are” for two-factor authentication to in-person services.

The provincial identity information services provide the capabilities to use the BC Services Card for these types of authentication, including managing the identity information and passcode associated with the card.

A passcode is a secret numeric password that can be used with a card to authenticate an individual, similar to a PIN with a bank or credit card. The passcode is associated to an individual’s card and is not specific to or exposed to any online service that uses it.

2.2. BC Services Card Program

2.2.1. Background

The BC Services Card Program is an integrated program between the Ministry of Health (Health), the Insurance Corporation of British Columbia (ICBC) and the Ministry of Technology, Innovation and Citizens' Services (MTICS). The program was established through a multi-year project to develop and issue a high quality card to BC residents to replace Health's Care Card used for provincial health insurance.

In 2012, the partnership was formed in order to leverage the respective strengths and mandates of each organization. Through the administration of the Medical Services Plan (MSP), Health has the most comprehensive client base (99%) in the BC public sector. Health began planning and analysis in 2009 to issue a new photo card with a chip and expiry date. The Deputy Minister's Council for Transformation and Technology recognized that the new Care Card initiative could be linked to the corporate Government 2.0 Strategy: Citizens @ the Centre and the Office of the CIO's IM/IT Enablers. Health was directed to work with MTICS who would create the infrastructure for a corporate identity information management system. Lastly, strategic direction was provided to leverage ICBC's province-wide infrastructure, technology and best practices for in-person identity proofing for the purpose of issuing a BC Services Card to all British Columbians who are enrolled in MSP.

The partners established the primary objectives of the first phase project as:

1. Enhance privacy protections;
2. Ensure the delivery of government services to the right person;
3. Create a card that may be used for other government services;
4. Leverage existing driver licencing offices and secure identity information practices;
5. Reduce consumer fraud resulting from Care Card misuse; and
6. Reduce identity theft resulting from Care Card misuse.

2.2.2. Integrated Program Agreement

The partners have signed an integrated program agreement that clearly establishes the service provided and information sharing agreements between the organizations, and the key objectives and expected benefits including:

- To issue a high assurance card which can be used to prove one's identity for the purpose of accessing multiple services across government;
- To set the foundation for secure and trusted online access to high value services and information;
- To issue and renew the card in a manner that maximizes convenience for citizens;
- To ensure security and privacy protection through the use of advanced chip technology and privacy enhancing system architecture;
- To leverage investments in high quality and trusted identity proofing infrastructure, technology and processes; and,
- To manage and reduce incidents of identity and eligibility fraud.

The partners work collaboratively together to provide services related to:

- BC Services Card issuance, replacement and renewal;
- Identity proofing;
- Verifying MSP eligibility;
- Confirming BC residency;
- Card production and delivery;
- Chip activation and deactivation;
- Identity fraud management;
- Notification to individuals about renewals; and,
- Recovery of lost/stolen/cancelled cards.

MTICS holds the authority under the authority of s. 69.2 of the *FOIPP Act* for issuing the BC Services Card, except for the Combo card which is co-issued by ICBC under the authority of the *Motor Vehicle Act*.

Each partner organization uses service delivery partners and service providers to deliver their programs, as follows.

- The partnership uses Service BC for call centre services to support individuals with inquiries about the card.
- Ministry of Health uses Health Insurance BC (HIBC) for delivering the provincial health insurance program.
- ICBC uses IBM for facial recognition and card production services and IRIS for card manufacturing.
- ICBC uses Service BC and appointed agents for delivering driver licensing and BCID programs in locations where ICBC does not have its own offices.
- The IDIM Program uses SecureKey Technologies Inc. to support chip management and authentication services, card reader supply and advanced technical support relevant to chip authentication.

The following overview diagram illustrates the partner organizations and their key responsibilities and interactions to deliver the BC Services Card to individuals (specifically, the combo or photo card issuance flow is illustrated).

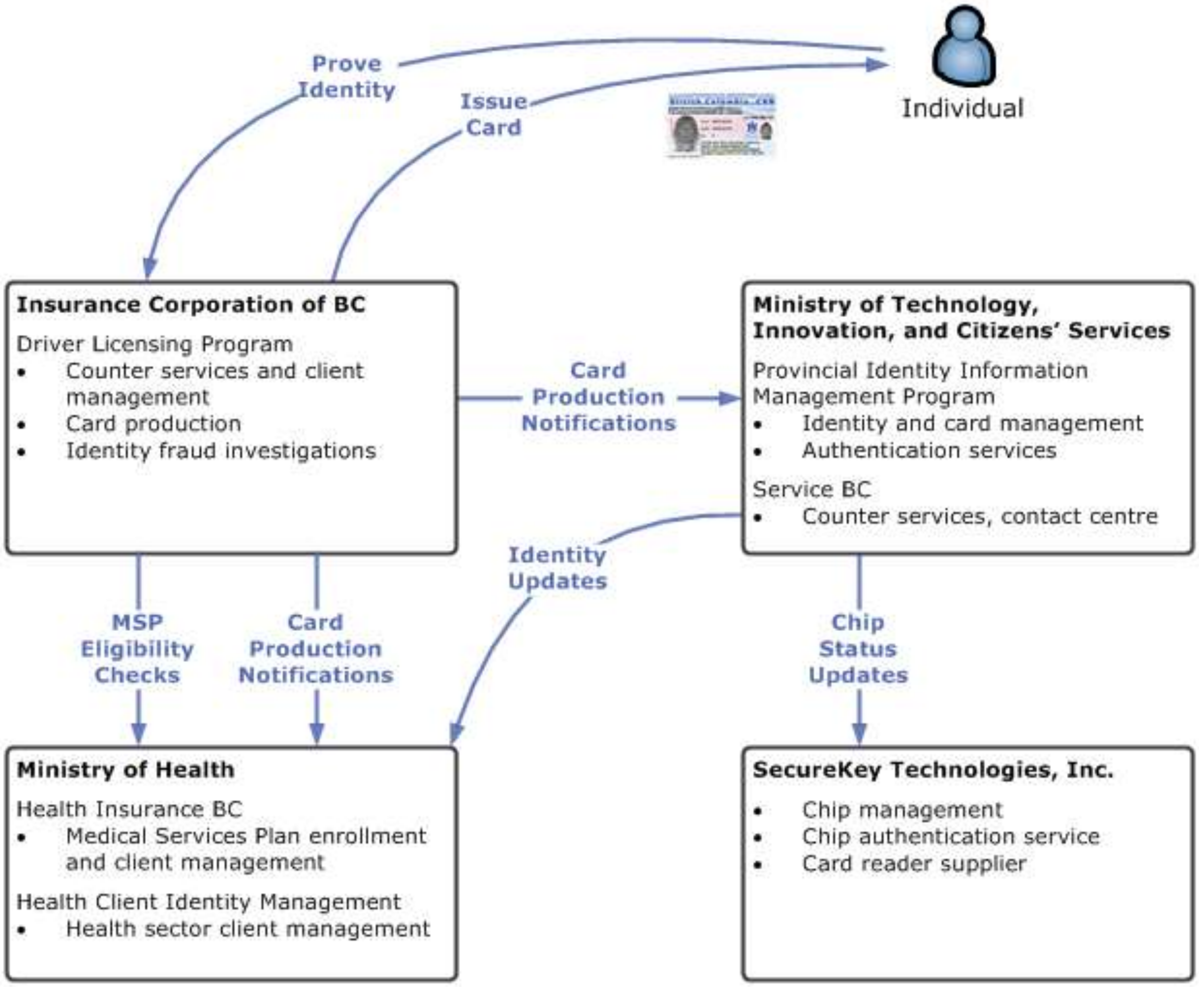

Prove Identity
Issue Card
Individual
Insurance Corporation of BC
Driver Licensing Program
• Counter services and client management
• Card production
• Identity fraud investigations
Card Production Notifications
Ministry of Technology, Innovation, and Citizens' Services
Provincial Identity Information Management Program
• Identity and card management
• Authentication services
Service BC
• Counter services, contact centre
Identity Updates
MSP Eligibility Checks
Card Production Notifications
Chip Status Updates
Ministry of Health
Health Insurance BC
• Medical Services Plan enrollment and client management
Health Client Identity Management
• Health sector client management
SecureKey Technologies, Inc.
• Chip management
• Chip authentication service
• Card reader supplier

Figure 3: BC Services Card Program Overview of Card Issuance

ICBC's driver licensing program is responsible for handling card requests and identity proofing individuals in support of issuing the BC Services Card. Ministry of Health confirms that the individual is eligible for the Medical Serivces Plan and updates its records for health insurance purposes. ICBC sends notification to MTICS about cards that are produced so that it can establish identity records for use in its authentication services. MTICS also provides up to date identity information to Ministry of Health for its client identiy management system.

MTICS has contracted SecureKey Technologies, Inc. to supply the chip data embedded in the BC Services Card, provide authentication services on personal computers, tablets and smartphones, and supply card readers for personal computers.

2.3. Provincial IDIM Program

The Provincial Identity Information Management (IDIM) program is a branch of the Ministry of Technology, Innovation and Citizens' Services (MTICS) under the Division of the Office of the Chief Information Officer (OCIO). The IDIM program is the organization unit of MTICS that is responsible for the MTICS partnership of the BC Services Card program.

2.3.1. Provincial Identity Information Services Provider

The IDIM program is also the organization unit responsible on behalf of MTICS to be the Provincial Identity Information Services Provider (PIISP), as per s. 69.2 of the *Freedom of Information and Protection of Privacy (FOIPP) Act*. The Minister responsible for the *FOIPP Act* has designated MTICS as the PIISP to provide the following identity information management services, as is written in s. 69.2 (2):

> *A provincial identity information service provider, by exercising its powers respecting the collection, use and disclosure of information, may provide the following services:*
>
> *(a) identifying an individual;*
>
> *(b) verifying the identity of an individual;*
>
> *(c) updating personal identity information about an individual;*
>
> *(d) issuing a physical or an electronic credential to an individual;*
>
> *(e) managing the information associated with a physical or an electronic credential;*
>
> *(f) any other service related to personal identity information that the minister responsible for this Act considers appropriate.*

The PIISP is required to comply with the directions issued by the Minister that ensure a high standard of security and privacy protection for the personal identity information in its custody or under its control.

2.3.2. Provincial Identity Information Services

The IDIM Program has set a strategic direction to provide centralized identity management and authentication services for government. It has the goals of:

- improving identity assurance across government to support delivering the right services to the right people;
- enabling higher valued services to be put online; and,
- improving online service delivery by providing new and better ways to identify users.

The IDIM Program has several existing services and is continuing to develop and evolve services to fulfill its mandate. Existing services include identity management of government workers (IDIR), citizens and businesses (BCeID), and web access management to enable online service delivery.

To support its role in the BC Services Card initiative, the IDIM Program established a foundational identity platform system called the Identity Assurance Services (IAS). With the IAS, the IDIM Program can manage identity and card information about BC Services Cards and provide card authentication services to support government programs and services.

The following overview diagram illustrates the IDIM Program's focus on BC Services Card authentication services, where it is a service provider to government ministries.

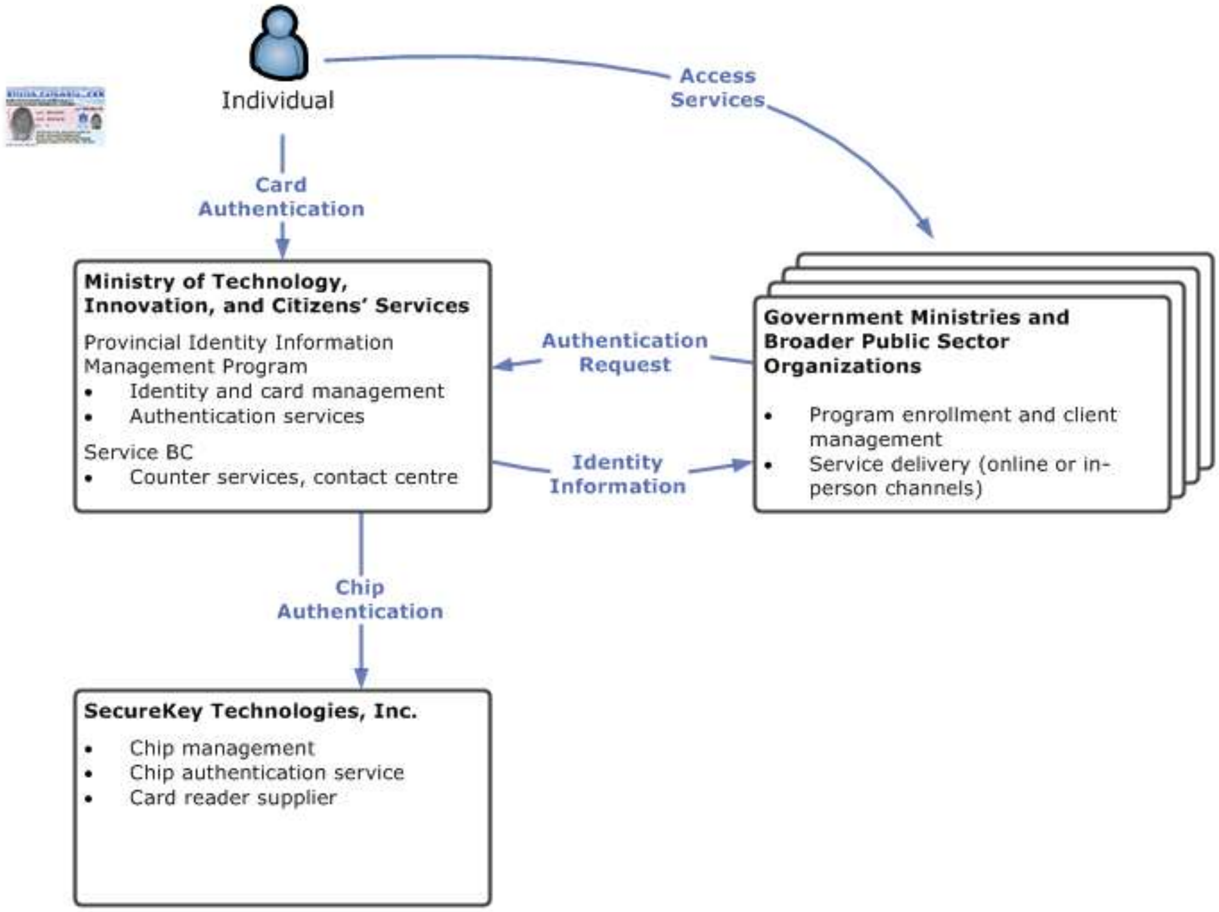

Individual
Access Services
Card Authentication
Ministry of Technology, Innovation, and Citizens' Services
Provincial Identity Information Management Program
• Identity and card management
• Authentication services
Service BC
• Counter services, contact centre
Authentication Request
Identity Information
Government Ministries and Broader Public Sector Organizations
• Program enrollment and client management
• Service delivery (online or in-person channels)
Chip Authentication
SecureKey Technologies, Inc.
• Chip management
• Chip authentication service
• Card reader supplier

Figure 4: IDIM Program Overview on BC Services Card Authentication Services

2.3.3. Principles

The IDIM Program develops its services and policies in alignment with the following sets of principles. The first set of principles was developed as part of the pan-Canadian Identity Management and Authentication Taskforce in 2006.

1. Identity information requirements and uses should be justifiable and proportionate to the task.
2. Clients (individuals) should have choice, consent and control over their identity credentials and the uses to which they are put.
3. Use of identity information should be limited to a specific purpose and to justifiable parties.
4. Identity information management processes should be client-focused and provide a consistent experience.
5. An identity information management environment should recognize a diversity of identity contexts and systems.
6. Identity information management should be provided in a trusted and secure environment.
7. All identity information management activities should be transparent and accountable.
8. Identity information management processes and methods should provide an enduring solution, which is technologically neutral, flexible and scalable.

During the concept phase of the IDIM initiative in 2008, the following solution design principles were developed.

1. Privacy: The solution must meet current privacy standards, and enhance privacy protection of identity information.
2. Security: The solution must use security best practices employing least privilege, defense in depth, and threat modelling methodologies.
3. Information Sharing: The solution must enable authorized information sharing within and across information domains and adhere to proportionality.
4. Citizen-centric: The solution must create and provide user choice and control.
5. Efficiency and Practicality: The solution should leverage previous IDIM work and existing assets wherever possible. Ideally, it would be delivered within existing legislation and provide value to in-flight projects.

2.3.4. Identity Assurance Model

The IDIM Program is guided by several reference models that were established during the concept phase of the IDIM initiative. The most notable one is the Identity Assurance Model.

Identity assurance is a measure of confidence that an identity attribute or set of attributes is true. It is measured in levels which indicate strength of the assurance that can be placed in these attributes. The higher the level of assurance the higher degree of certainty in identity attributes.

Transaction assurance is a pre-determined level of certainty in identity attributes that applies to a transaction or service. Organizations responsible for services must determine the appropriate transaction assurance levels by examining the sensitivity of the information involved. The transaction level dictates the Identity Assurance Level.

The Identity Assurance Model is a model based on a four level framework that describes Identity Assurance Levels, their relationship to Transaction Assurance Levels and their dependency on registration processes, credential strength, authentication events and the underlying operational infrastructure and processes.

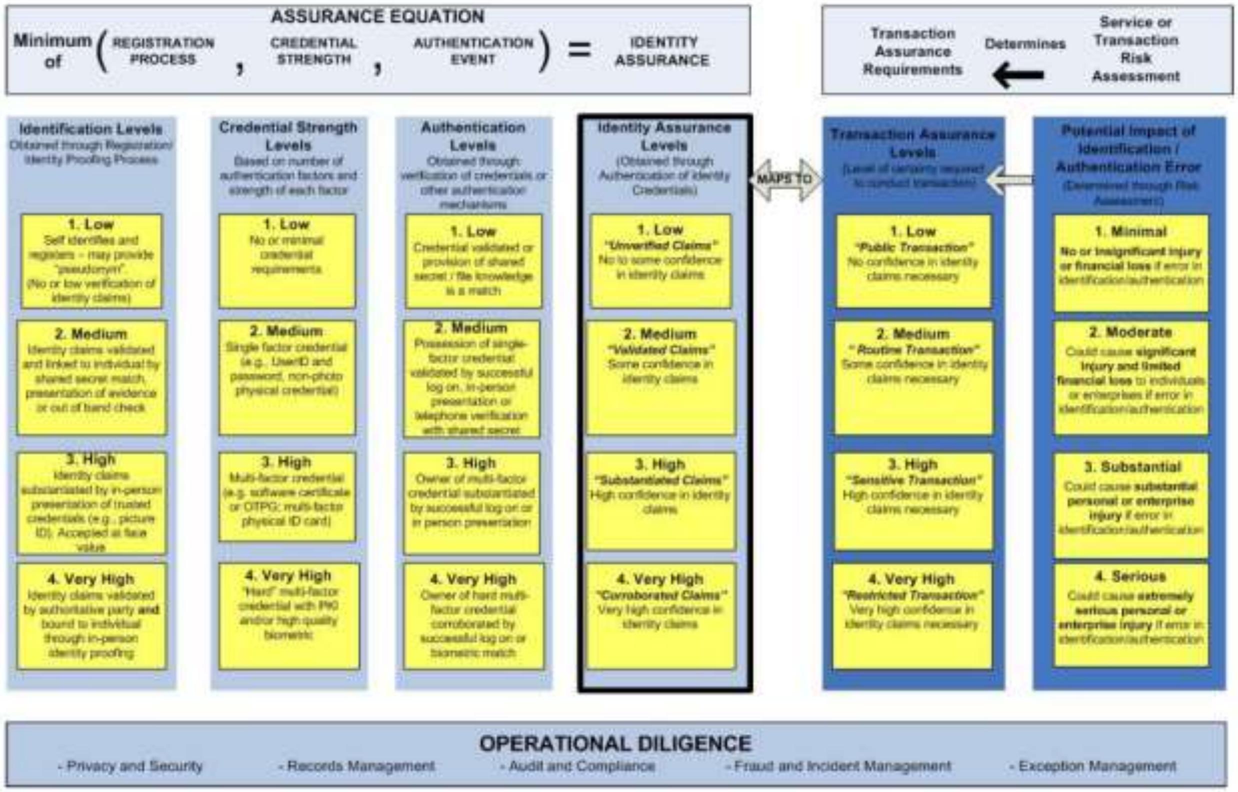

ASSURANCE EQUATION
Minimum of (REGISTRATION PROCESS , CREDENTIAL STRENGTH , AUTHENTICATION EVENT) = IDENTITY ASSURANCE
Transaction Assurance Requirements
Determines
Service or Transaction Risk Assessment
Identification Levels
Obtained through Registration/ Identity Proofing Process
1. Low
Self identifies and registers – may provide "pseudonym". (No or low verification of identity claims)
2. Medium
Identity claims validated and linked to individual by shared secret match, presentation of evidence or out of band check
3. High
Identity claims substantiated by in-person presentation of trusted credentials (e.g., picture ID). Accepted at face value
4. Very High
Identity claims validated by authoritative party and bound to individual through in-person identity proofing
Credential Strength Levels
Based on number of authentication factors and strength of each factor
1. Low
No or minimal credential requirements
2. Medium
Single factor credential (e.g., UserID and password, non-photo physical credential)
3. High
Multi-factor credential (e.g. software certificate or OTPG; multi-factor physical ID card)
4. Very High
"Hard" multi-factor credential with PKI and/or high quality biometric
Authentication Levels
Obtained through verification of credentials or other authentication mechanisms
1. Low
Credential validated or provision of shared secret / file knowledge is a match
2. Medium
Possession of single-factor credential validated by successful log on, in-person presentation or telephone verification with shared secret
3. High
Owner of multi-factor credential substantiated by successful log on or in person presentation
4. Very High
Owner of hard multi-factor credential corroborated by successful log on or biometric match
Identity Assurance Levels
(Obtained through Authentication of Identity Credentials)
1. Low
"Unverified Claims"
No to some confidence in identity claims
2. Medium
"Validated Claims"
Some confidence in identity claims
3. High
"Substantiated Claims"
High confidence in identity claims
4. Very High
"Corroborated Claims"
Very high confidence in identity claims
MAPS TO
Transaction Assurance Levels
(Level of certainty required to conduct transaction)
1. Low
"Public Transaction"
No confidence in identity claims necessary
2. Medium
" Routine Transaction"
Some confidence in identity claims necessary
3. High
"Sensitive Transaction"
High confidence in identity claims necessary
4. Very High
"Restricted Transaction"
Very high confidence in identity claims necessary
Potential Impact of Identification / Authentication Error
(Determined through Risk Assessment)
1. Minimal
No or insignificant injury or financial loss if error in identification/authentication
2. Moderate
Could cause significant injury and limited financial loss to individuals or enterprises if error in identification/authentication
3. Substantial
Could cause substantial personal or enterprise injury if error in identification/authentication
4. Serious
Could cause extremely serious personal or enterprise injury if error in identification/authentication
OPERATIONAL DILIGENCE
- Privacy and Security
- Records Management
- Audit and Compliance
- Fraud and Incident Management
- Exception Management

Figure 5: Identity Assurance Model

Government programs must use this model to determine the required identity assurance levels for the transactions they offer. Once the transaction assurance levels have been established, the appropriate BC Services Card credential types can be identified.

The following table lists how the three types of BC Services Card, when combined with a passcode or not, provide different levels of assurance when used electronically. When government programs and services require the use of the combo or standalone photo BC Services Card with a passcode to access their services, they can have **high** confidence that the individual is who they claim to be.

Table 1: BC Services Card Identity Assurance Levels

BC Services Card Credential	Identification Level	Credential Strength Level	Authentication Level	Identity Assurance Level
Photo Card with Passcode	High	High	High	**High**
Combo Card with Passcode	High	High	High	**High**
Non-Photo Card with Passcode	Low	High	High	Low
Photo Card without Passcode	High	Medium	Medium	Medium
Combo Card without Passcode	High	Medium	Medium	Medium
Non-Photo Card without Passcode	Low	Medium	Medium	Low

2.4. Identity Assurance Services Overview

The Identity Assurance Services (referred to as the IAS) is the foundational system to support the BC Services Card and provide identity information services.

The purpose of the IAS is to securely manage the registered personal identity information and electronic credentials for individuals who interact with government services. The IAS is also the service provider that authenticates the electronic credentials and provides identity information to relying government programs and services to help them to deliver their services to their clients.

The following diagram illustrates the major systems of each partner organization and service provider with focus on the IAS as the central system supporting the BC Services Card program. The IAS, each system and the interactions between them will be described in detail in this document.

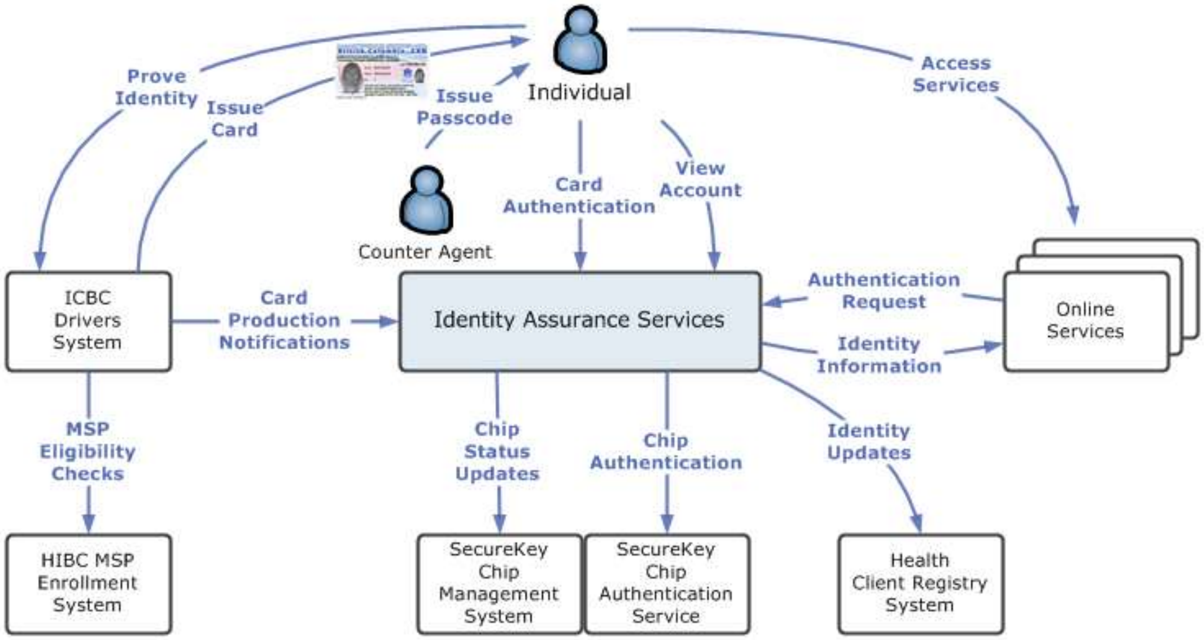


Figure 6: IAS Solution Context

The IAS registers and manages information about individuals who are issued cards by ICBC. It also registers information about the cards and forwards chip status information to SecureKey so that it can activate the chip for use. As part of the card issuance process, IAS also forwards identity information to the Health Client Registry so they have up-to-date information for healthcare service delivery.

When an individual uses their BC Services Card to access an online service, they interact with the IAS to authenticate their card in order to allow the IAS to provide their identity information to the online service. The IAS interacts with SecureKey using their Chip Authentication Service that verifies chip data to determine that it is authentic.

To achieve high identity assurance, individuals require a passcode to use with their card, which meets the two-factor authentication model. Passcodes can be issued through an authorized counter agent of government; for the initial rollout of the solution this is delivered by Service BC at locations throughout British Columbia; Service BC is a government service delivery organization of MTICS.

The IAS is being developed to support an in-person authentication capability, where an individual can use the IAS to authenticate their card and prove their identity for services delivered in face-to-face transactions.

2.5. Business Scenarios

The IAS solution architecture is described throughout this document arranged by the following key business processes that involve the BC Services Card and the Identity Assurance Services:

1. Card Issuance
2. Online Authentication
3. Passcode Issuance
4. Account Management
5. Onboarding and Support

2.5.1. Card Issuance

The BC Services Card program has the responsibility to issue cards to BC residents. The IAS is one of several systems involved in the card issuance process.

Combo/Photo Card Issuance
The process of issuing a combo or photo standalone card to an individual begins with their card request and identity proofing event at a driver licensing office.

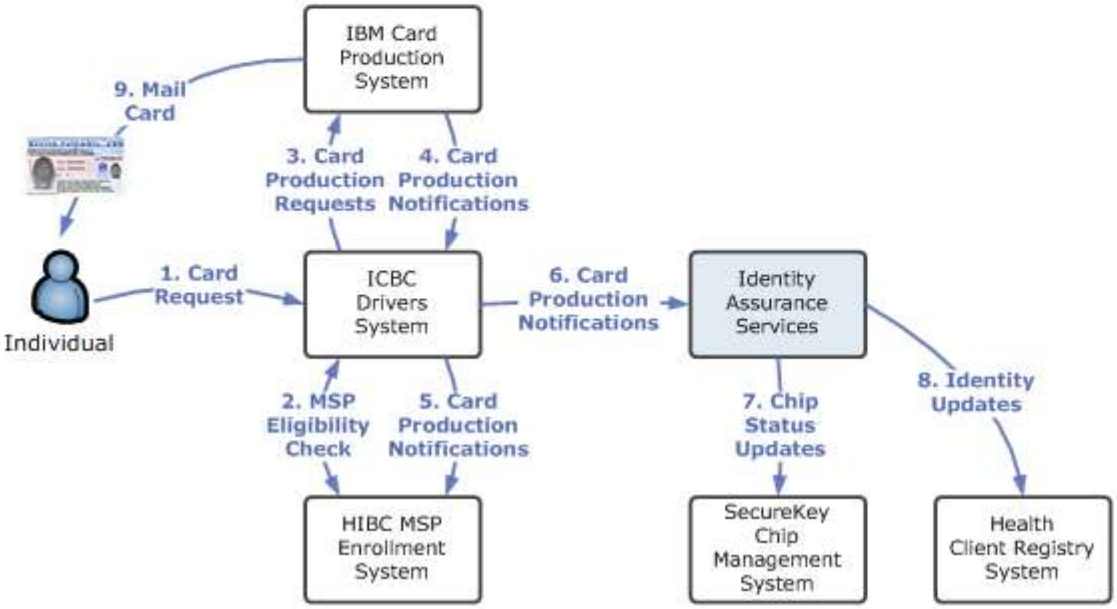

IBM Card Production System
9. Mail Card
3. Card Production Requests
4. Card Production Notifications
Individual
1. Card Request
ICBC Drivers System
6. Card Production Notifications
Identity Assurance Services
8. Identity Updates
2. MSP Eligibility Check
5. Card Production Notifications
7. Chip Status Updates
HIBC MSP Enrollment System
SecureKey Chip Management System
Health Client Registry System

Figure 7: Combo/Photo Card Issuance

ICBC is responsible for the counter service that involves identity proofing the individual, checking their MSP eligibility with HIBC, taking a photograph of the individual and handling payment for driver's licence fees. ICBC verifies the individual is unique using its facial recognition system, then requests that a card be produced and mailed by IBM, its service provider. Once a card has been produced (printed and registered), ICBC notifies HIBC and MTICS. HIBC uses this notification to complete the individual's enrollment or re-enrollment in MSP. MTICS uses this notification to register identity and card data in the IAS, activate the chip with SecureKey and provide updated client identity information to Health.

Non-Photo Card Issuance

The process of issuing a non-photo card to an individual typically begins with their card request direct to HIBC through their call centre. Non-photo cards are also automatically issued for children after a newborn birth registration, and are sometimes issued to children after their parent(s) obtain a card.

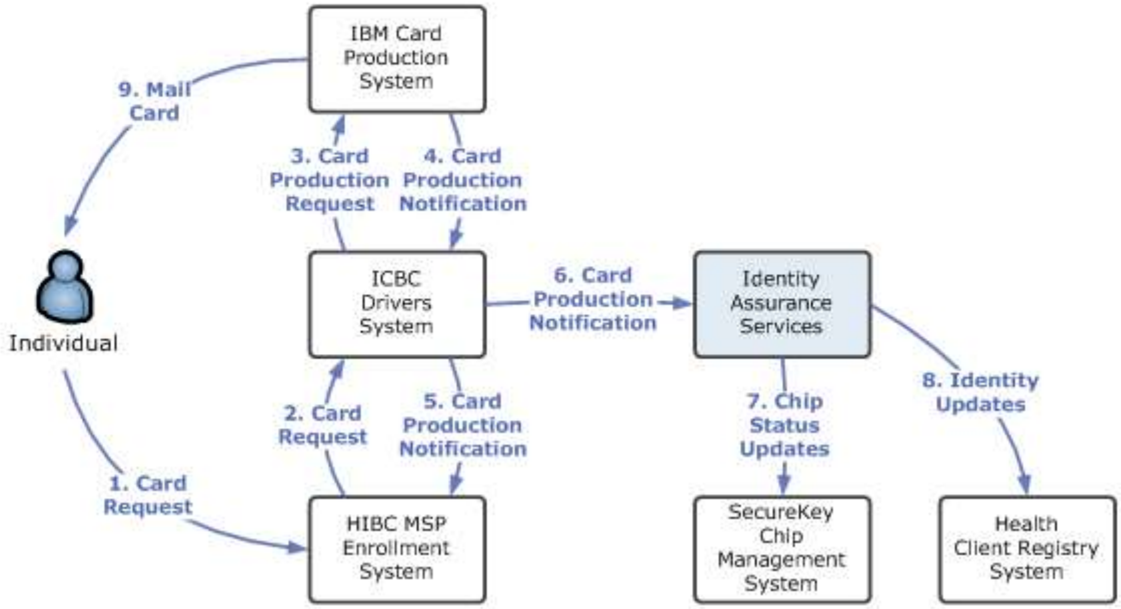

IBM Card Production System
9. Mail Card
3. Card Production Request
4. Card Production Notification
Individual
ICBC Drivers System
6. Card Production Notification
Identity Assurance Services
2. Card Request
5. Card Production Notification
7. Chip Status Updates
8. Identity Updates
1. Card Request
HIBC MSP Enrollment System
SecureKey Chip Management System
Health Client Registry System

Figure 8: Non-Photo Card Issuance

HIBC is responsible for the call centre service that receives card requests and determines whether the requester meets the exemption or exception criteria to receive a non-photo card (e.g. children, elderly, health conditions that restrict counter visits). HIBC confirms the individual through knowledge-based authentication and checks their MSP eligibility, then requests that ICBC produce a non-photo card. ICBC registers the non-photo card requester as a client, then triggers a card to be produced and mailed by IBM. Once a card has been produced (printed and registered), ICBC notifies HIBC and MTICS. MTICS uses this notification to register identity and card data in the IAS, activate the chip with SecureKey and provide updated client identity information to Health.

Card Manufacturing
There is also a back office process to order and manufacture cards that provides inventory for daily card production by IBM.

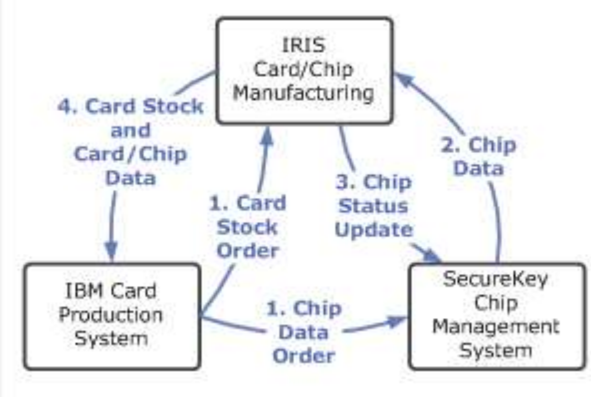

IRIS Card/Chip Manufacturing
4. Card Stock and Card/Chip Data
1. Card Stock Order
3. Chip Status Update
2. Chip Data
IBM Card Production System
1. Chip Data Order
SecureKey Chip Management System

Figure 9: Card Manufacturing

On a monthly basis, IBM requests more inventory to be prepared by sending a request to IRIS to manufacture blank card stock and to SecureKey to prepare chip data for that card stock. SecureKey generates chip data with its keys and securely provides chip data to IRIS to use to fulfill the card order. IRIS notifies SecureKey after the chips have been prepared so that SecureKey can update the chip status in its system. IRIS securely delivers the physical card stock to IBM, and also provides IBM with the card and chip data including the unique card serial numbers and chip numbers for IBM inventory management.

Card Renewals and Replacements
Cards are issued with an expiry date; an individual is required to request a renewal card in the same manner as they obtained their previous card - through a counter visit with ICBC or a telephone call to HIBC. For combo/photo cards, the expiry date aligns with driver's licence expiry or the individual's birthdate two or five years in the future. For non-photo cards, the expiry date aligns with the individual's birthdate five years in the future or a child's 19th birthday when they must obtain a combo/photo card.

Individuals sometimes need replacement cards, such as when their card is lost, stolen or damaged. An individual is required to request a replacement card in the same manner as they obtained their previous card - through a counter visit with ICBC or a telephone call to HIBC. For combo/photo cards, each replacement and renewal card request requires identity proofing the individual, taking a new photograph and verifying the individual using its facial recognition system.

Each system of ICBC, HIBC and MTICS registers identity and every card that is issued. Health Client Registry updates each identity but does not register cards. SecureKey updates each chip but does not contain identity information.

2.5.2. Online Authentication

The IDIM Program has the responsibility to provide BC Services Card authentication services to BC residents for access to government services. The IAS is the system that provides authentication and identity information to government online services.

Login with Card and Passcode

The process of authenticating a user for an online service is also commonly referred to as the login process. It begins when an individual requests access to an online service through a login or register button.

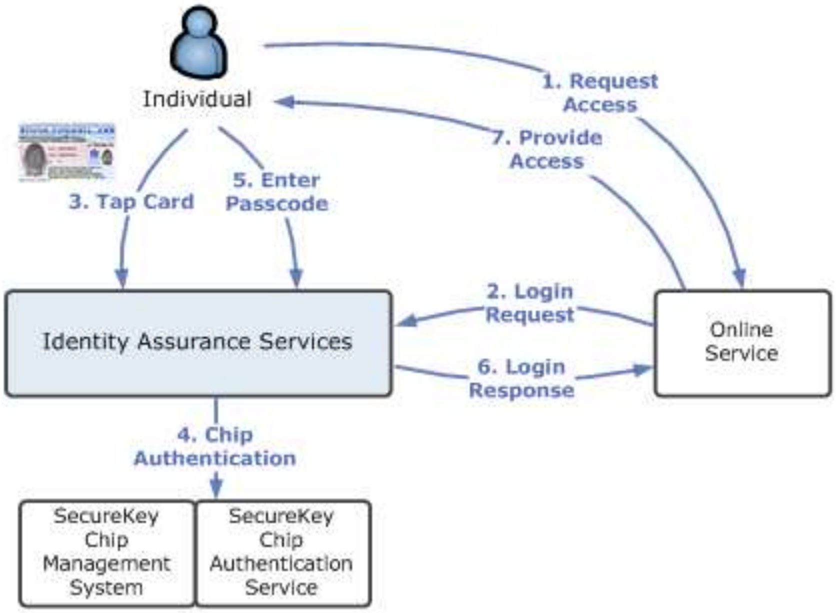


Figure 10: Login with Card and Passcode

When an online service receives a request by an individual to login, the online service then makes a login request to the IAS to start the login process. The IAS facilitates the login process by prompting the individual to tap their card on their card reader; then the IAS requests to SecureKey to authenticate the chip, which involves verifying the chip data and checking the chip status. A successful chip authentication will determine the unique identity that was registered to the card, from which the IAS can check the status of the card, and then prompt for and validate the passcode corresponding to the card. If the individual authenticates successfully, they may confirm their specific identity information to be provided from the IAS to the online service.

The IAS provides an identifier and identity attributes about the individual to the online service, as well as the identity assurance level achieved by the login process. The identity attributes are sourced from the identity information that was registered when the card was issued. The online service can use this data to register or match the individual's identity information in its system, determine what the individual is authorized to access, and then provide its information or services to that individual.

Through this login process, the online service receives only those identity attributes about the individual that it is configured to receive, not all identity attributes and not specific details about the card or passcode used.

2.5.3. Passcode Issuance

The IDIM Program has the responsibility to issue passcodes to BC residents for their use with their BC Services Card for online authentication. It is expected that an individual will request a passcode when they are motivated to start using online services with their card. In the future, passcodes may be provided at the same time cards are issued.

The IDIM Program has a service agreement with Service BC to provide the counter service to issue passcodes. The IAS is the system that manages passcode data and the application that counter agents use to issue the passcodes.

Passcodes Issuance for Combo/Photo Cards
The process of issuing a passcode to an individual with a combo or photo standalone card begins with a request at an authorized government service counter location.

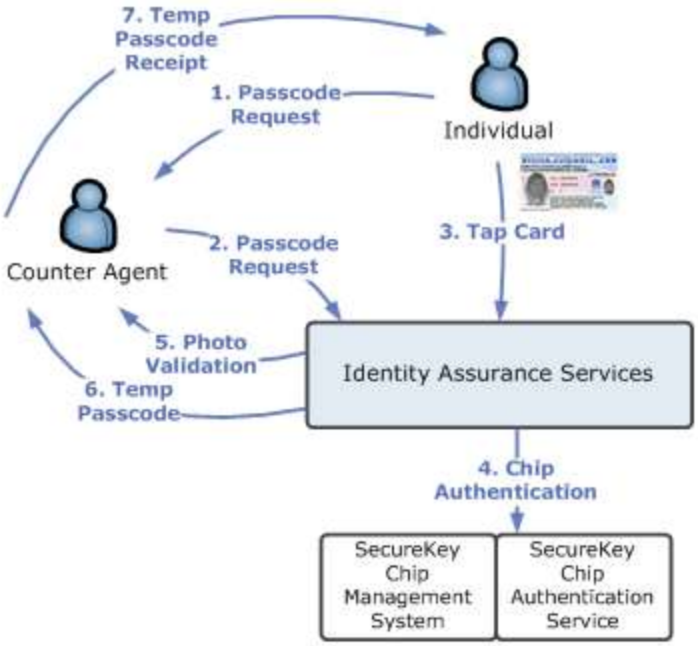


Figure 11: Passcode Issuance

The counter agent is responsible for identifying the individual using card authentication and validating that the photo in the system matches the individual standing before them. When a counter agent receives an individual with a request for a passcode, the agent will use the IAS to facilitate the process by prompting the agent to have the individual tap their card on the counter card reader. The IAS then sends a request to SecureKey to authenticate the chip, which involves verifying the chip data and checking the chip status.

A successful chip authentication will determine the unique identity that was registered to the card, from which the IAS can check the status of the card, and then present the photo of the registered individual for validation by the counter agent. If the counter agent determines the individual matches their registered photo, they are provided with a temporary passcode on a printed receipt.

The individual is instructed to access an online service with their BC Services Card within the time period before the temporary passcode expires (one week). The IAS will prompt the individual to enter their temporary passcode during the login process, and then ask the individual to set a new passcode for ongoing use.

Passcodes Issuance for Non-Photo Cards
There is a simpler, though less secure, way to establish a passcode for a non-photo card. A passcode does not need to be issued to an individual with a non-photo card; rather the individual may set their own passcode the first time they use the card in a login process.

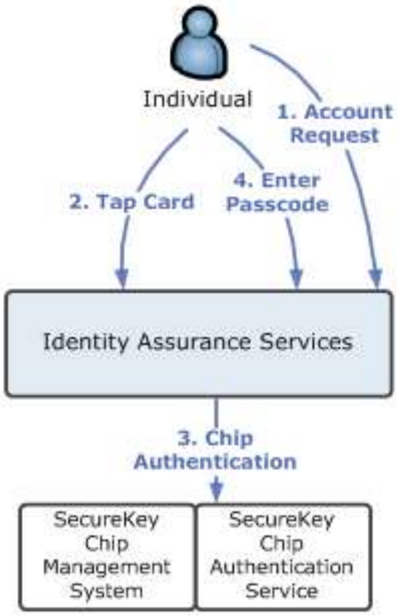

Individual
1. Account Request
2. Tap Card
4. Enter Passcode
Identity Assurance Services
3. Chip Authentication
SecureKey Chip Management System
SecureKey Chip Authentication Service

Figure 12: Passcode Setting for Non-Photo Cards

The individual may set their own passcode through login to either their IAS account or an online service that accepts non-photo cards. The IAS facilitates the login process by prompting the individual to tap their card on their card reader and requesting SecureKey to authenticate the chip, which involves verifying the chip data and checking the chip status.

A successful chip authentication allows the IAS to determine the unique identity that was registered to the card, from which the IAS can check the status of the card, determine whether it is the first time and that the card type is non-photo, and then prompt for the individual to set a new passcode for ongoing use.

Passcodes Resets
An individual can change their passcode if they know their current one, however it is anticipated that individuals will forget their passcode and need to have it reset, especially if they do not often use their BC Services Card to login to online services.

An individual with a combo/photo card is required to reset their passcode in the same secure manner of an in-person counter visit. They will need to tap their card, have their photo validated and receive a printed receipt with a temporary passcode. This process ensures that the individual requesting the passcode reset is the intended card holder. A passcode for a combo/photo card cannot be reset over the phone or via email.

An individual with a non-photo card has the option to provide an email address for a simpler, though less secure, way to reset their passcode. During the login process, after the individual has tapped their card on their card reader and the card is successfully authenticated, the individual may indicate that they forgot their passcode which triggers the IAS to send an email to the registered email address with a temporary passcode. The individual may use that immediately in the login process, then will be prompted to set a new passcode for ongoing use. If the individual does not use email, or forgets their email password, or doesn't use that email account anymore, they need to have an in-person counter visit to reset their passcode.

Card Readers
Individuals may use a small card reader device to connect to their computer on which to tap their card for the login process. The IDIM Program is procuring these card readers, and authorized government service counters will help distribute these to individuals. Card readers are not electronically assigned to an individual; they may be safely shared within a family or household.

Counter agents also require counter card reader devices to connect to their computers on which to allow individuals to tap their cards for the passcode issuance process. The IDIM Program is also responsible for procuring these card readers and distributing to authorized service counter locations for their use.

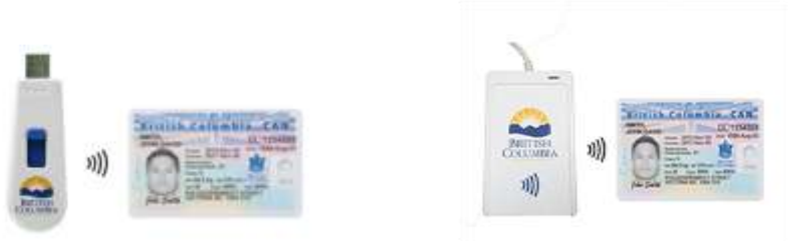


Figure 13: USB and Counter Card Readers

Mobile Devices
Individuals may also use an Android mobile device (smartphone or tablet) as a card reader. To act as a card reader, the Android device must be capable of Near Field Communications (NFC) and have the BC Services Card Mobile Application installed. This application is available to be downloaded from the Google Play Store.

2.5.4. Account Management

The IDIM Program provides an online BC Service Card account for individuals with a BC Services Card. The IAS is the system that manages the account sourced from the identity and card information that was registered when the card was issued. The account also supports the individual by providing a history view of how they've used their card and changes to their account.

The individual is required to login with their card and passcode in order to access their account. The individual may perform several basic functions within their account:

- View their registered identity information
- Change their passcode
- Change their email address
- Change their login or other account preferences
- View their account history, which includes when card(s) were issued, when passcodes were changed, and when cards were used for online authentication.

The IDIM program also receives notifications about address changes from ICBC on a regular basis. Address updates are applied directly to an individual's account.

2.5.5. Onboarding

The process of onboarding a government program with online services begins with providing overview information and facilitating an assessment of the program's identity management needs. This is followed up with consulting on the configuration options and the specific business and technical needs of the online service. This leads to a solution proposal, and may involve review and consulting by other staff in OCIO in areas such as policy, privacy, architecture, standards, and security.

Once there is agreement to move forward, the online service (when it is built and ready) must be configured in the IAS to integrate with its authentication services for the login process. This involves specifying the technical details of the online service and the identity attributes that it may receive about an authenticated user. Co-ordinated integrated testing is required to confirm that the integration is functioning in a test environment before the online service can be configured in the IAS for production use.

The IDIM Program also forms agreements with the government program about service support levels, cost recovery and information sharing. These agreements need to be in place before the online service is enabled for production use. The government programs also need to complete and submit a Privacy Impact Assessment and Security Threat Risk Assessment for review.

Onboarding Applications and Tools
The IDIM Program uses an application and common office software to track opportunities and manage contact information and agreements. However, the configuration profiles of online services are directly stored in IAS, as the configuration is needed to affect the login process at run-time.

2.5.6. Support

Support to Individuals
The IDIM Program uses a three-tier model for providing support to individuals. Tier 1 is the front-line contact point where requests for information and general assistance are provided. Tier 2 provides more in-depth support for a particular person's question or issue. Tier 3 provides support to Tier 2 on the most difficult issues or advanced technical or policy related inquiries.

Service BC provides Tier 1 call centre support for the BC Services Card program, including topics such as how to obtain a card, how to use get a passcode, and how to use a card to access an online service. The IDIM Program support staff provides Tier 2 and 3 support. For advanced technical issues involving card authentication, SecureKey provides key support to the IDIM Program.

Support to Online Service Providers
The IDIM Program also supports online service providers. The Shared Services BC Help Desk provides Tier 1 technical support to online service providers. The IDIM Program staff provides Tier 2 and 3 support to address technical and policy inquiries. For advanced technical matters involving card authentication, SecureKey provides support to the IDIM Program.

During the onboarding process, online service providers work directly with IDIM Program staff to resolve inquiries and issues related to onboarding activities.

Support Tools
The IDIM Program uses several third party tools to facilitate the support process, such as an incident management application to track support requests through to resolution. There are also several custom-built tools in the IAS for IDIM support staff, where there is a need for direct interaction with identity and card information within the IAS.

Support Websites
The IDIM Program and Ministry of Health provide a public website about the BC Services Card containing information about the card, how to use it for access to online services and how to get a passcode.

The IDIM Program also provides a public website about BC Services Card Onboarding intended for online service providers. This website contains information about the onboarding process and how the authentication service works.

3. SOLUTION ARCHITECTURE

This chapter provides an overview of the application, data, technology and security architecture of the Identity Assurance Services. It provides an overview and detailed description of each of the logical application groups, components and interfaces that accomplish the business scenarios described in chapter 2.

3.1. Application Architecture Overview

The application architecture of the IAS is described in terms of logical groups of application components, organized by commonality in the context of the key business scenarios. The four groups are:

1. Card Management
2. Core Data
3. Authentication
4. Support

The logical application groups and system interfaces are illustrated in the following diagram.

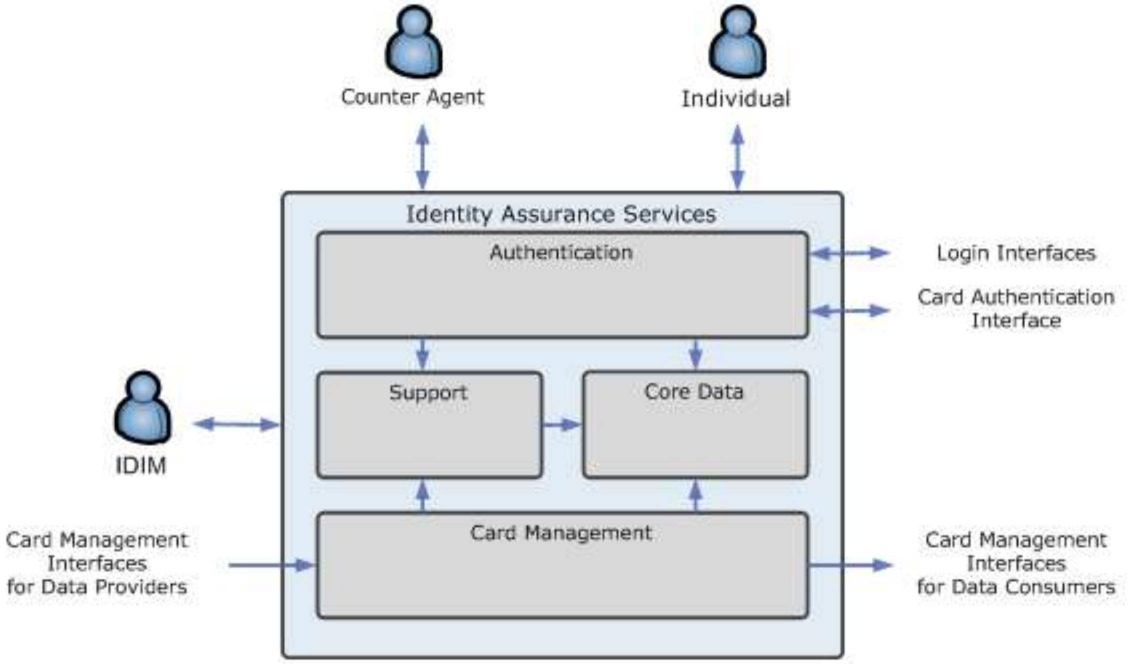

Counter Agent
Individual
Identity Assurance Services
Authentication
Login Interfaces
Card Authentication Interface
Support
Core Data
IDIM
Card Management
Card Management Interfaces for Data Providers
Card Management Interfaces for Data Consumers

Figure 14: IAS Application Groups

Each group of application components collaborate with other components to accomplish their functions. Some components provide user interfaces and system interfaces to external systems.

The following diagram elaborates the IAS overview presented earlier. It shows the main interactions between the IAS application groups, users and external systems, summarizing the business scenario diagrams presented in the previous chapter. (It is not intended to show all steps or all external systems involved in card issuance.)

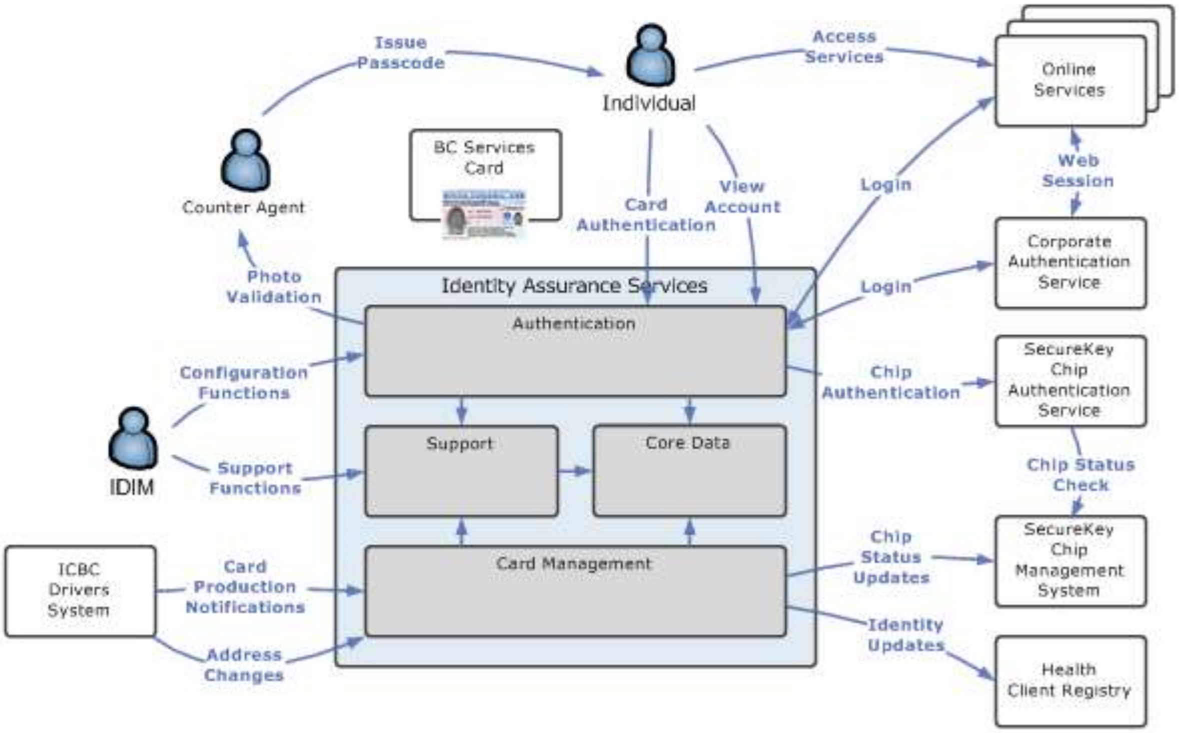


Figure 15: IAS Application Context Diagram

Each business scenario is accomplished using several IAS application components and may use one or more system interface to interact with external systems. The following table shows the mapping of business scenario to application groups and interfaces.

Table 2: Business Scenarios Application Mapping

Business Scenario	Application Group	User Interfaces	System Interfaces
1. Card Issuance	• Card Management • Core Data		• Card Management
2. Online Authentication	• Authentication • Core Data	• Individual	• Login • Chip Authentication • Mobile Application
3. Passcode Issuance	• Authentication • Core Data	• Counter Agent	• Chip Authentication

4. Self-Service	• Authentication • Core Data	• Individual	
5. IDIM Configuration and Support	• Support Tools • Authentication • Core Data	• IDIM Staff	

The Login interfaces of the IAS are a key part of the application architecture; they provide the methods to initiate and receive the results of the BC Services Card login process with the IAS. There are two interfaces in this category; each online service would use only one for its interaction with IAS:

1. SiteMinder Login
2. Federated Login using Security Assertion Markup Language (SAML)

The following diagram illustrates the two interface options and the application components involved.

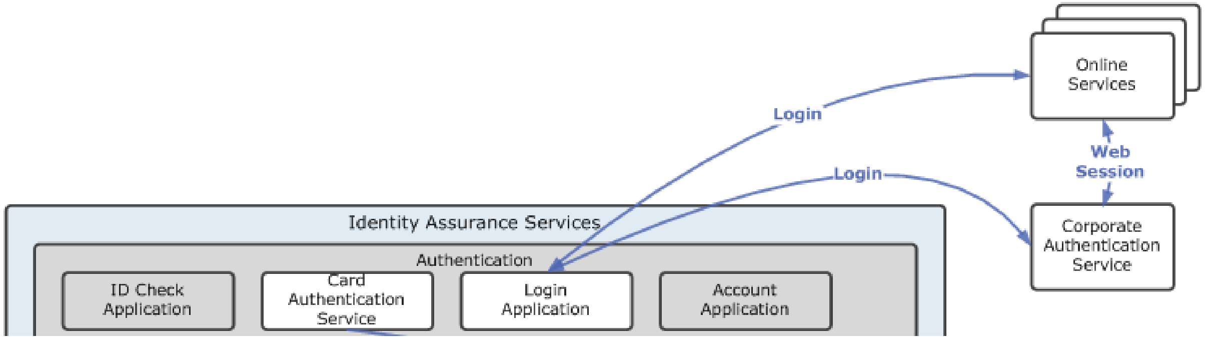


Figure 16: IAS Login Interfaces

Online Services

The Online Service component on the diagram represents a web-based information system that a government program operates in order to provide services to individuals. As an external system it is described generically in this document; its application architecture is not defined and varies widely across programs.

Generally, the Online Service is responsible to initiate login requests using one of the login interfaces, and receive the results of the login process. It is responsible to inform its users of the login process and how it will properly manage the identity information in accordance with government privacy and security policy.

Corporate Authentication Service

The Corporate Authentication Service is responsible for facilitating multiple types of login processes for government web applications, including web session management. In this context, it facilitates the card login process by interacting with IAS on behalf of an online service.

SiteMinder Login Interface

The SiteMinder Login interface provides the methods for initiating the login process with a SiteMinder protected web resource, and receiving the resulting identity attributes about the authenticated user through the SiteMinder web agent configured within the web server of the Online Service.

CA SiteMinder is a product that is implemented as part of government's Corporate Authentication Service. It is used by BC Government ministry information systems to orchestrate the login process for centrally managed user credentials and to provide web-based single sign-on and session management.

Login requests are initiated when an individual requests to access a SiteMinder-protected web resource. This is commonly represented to the individual as a login or registration button on the Online Service's website. The SiteMinder web agent in the Online Service's web server communicates with the centrally managed SiteMinder policy server to determine if the individual already has a web session, and if not it determines how to authenticate the user.

If the Online Service is configured to use BC Services Card, then SiteMinder redirects the individual to the IAS Login Application to go through the login process involving their card and passcode. After successful login, the IAS provides the identifier and identity attributes to SiteMinder; this uses the Federated Login interface described below. SiteMinder receives this information and then securely passes the data to the Online Service through its SiteMinder agent.

The Online Service receives the identifier and identity attributes and determines how to proceed. The Online Service can use this data to register or match the individual's identity information in its system, determine what the individual is authorized to access and then provide its information or services to that individual.

Federated Login Interface using SAML

The Federated Login interface provides the methods for initiating the login process using the industry standard federation approach called Security Assertion Markup Language (SAML). This standard specifies the messages and bindings for how an online service makes a request for login and receives identity information (called assertions) about the authenticated user after successful login.

The IAS provides the point-to-point interface for an Online Service to initiate the login process. Login requests are initiated when an individual requests to access a web resource on the Online Service's website. This is commonly represented to the individual as a login or registration button.

The Online Service sends a SAML login request to the IAS Login Application to facilitate the individual to go through the login process involving their card and passcode. After successful login, the IAS provides the identifier and identity attributes to the Online Service.

The Online Service validates the SAML login response provided by the IAS, receives the identifier and identity attributes, and determines how to proceed. The Online Service can use this data to register or match the individual's identity information in its system, determine what the individual is authorized to access and then provide its information or services to that individual.

Identifiers and Identity Attributes in Login Interfaces

The following lists some of the identity and login process data that may be provided to an Online Service, through either the SiteMinder or Federated Login interface.

- Surname, Given Names
- Birth Date, Age
- Street Address, Locality, Province, Postal Code
- Email Address
- Identity Assurance Level achieved by the login process
- Derived fields – for example "Age Over 19"

The identity attributes are sourced from the identity information that was registered when the card was issued. Which identity data is provided is based on information sharing agreements established during onboarding, and is determined from the profile in the Online Service Configuration service.

3.2. Data Architecture

The data architecture of the Identity Assurance Services is described in terms of the high level context of the IAS and external systems, and a description of how the IAS data is organized into several information domains.

The IAS is one of several systems that participate in the card issuance business scenario. The IAS stores and manages identity and card information provided by ICBC through the Card Production Notifications interface as described earlier. This identity and card information becomes the IAS core data upon which card authentication services are provided to government programs.

The following diagram illustrates the conceptual BC Services Card program information model; it shows that identity and card information is stored and managed in several systems across the BC Services Card program partners.

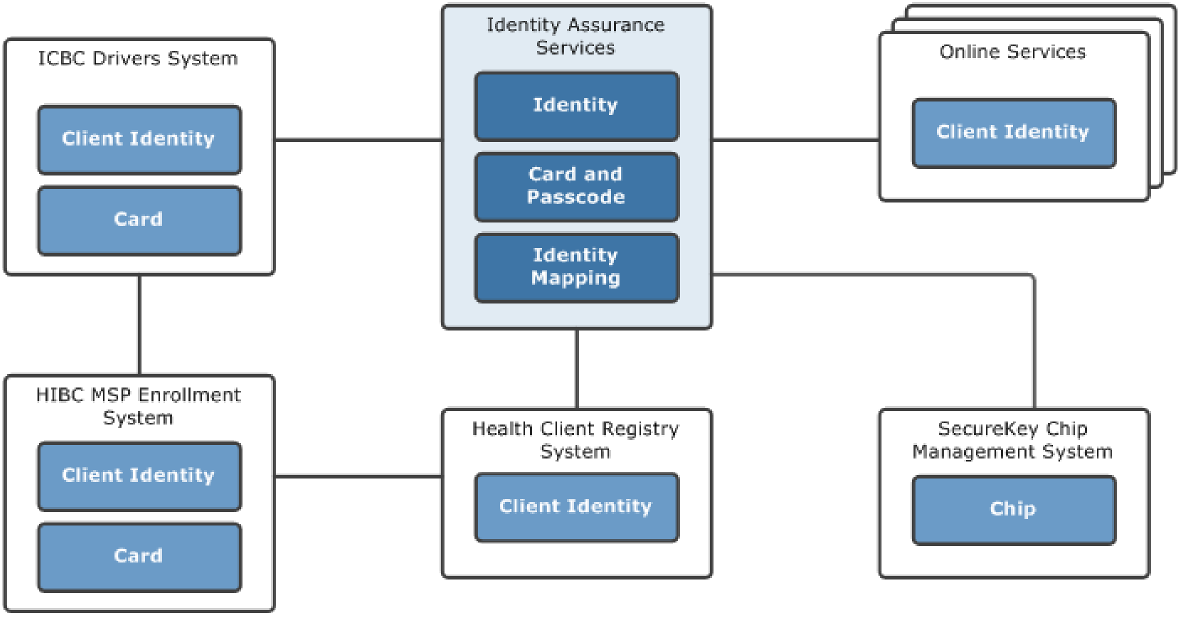


Figure 17: IAS Data Architecture Context

The ICBC Drivers System is considered to be the trusted data source for personal identity information and card information for all BC Services Cards, including the non-photo cards requested through HIBC.

Ministry of Health has two main data stores for their identity information: the HIBC MSP Enrollment System and the Health Client Registry System. HIBC stores identity and card information for all cards that are issued to associate with health insurance clients. The Health Client Registry is responsible for Personal Health Numbers and patient identity information; it does not store card information.

The IAS manages and stores the identity information associated with cards that are issued by ICBC, and stores the card information and its associated passcode. For each card registered in the IAS, there is an associated chip registered in the SecureKey Chip Management system. Both the IAS and SecureKey systems maintain the status of the card and chip, respectively. The IAS also maintains identity mappings of unique identifiers representing each identity for use with external systems and online services.

Each Online Service maintains the identity information, but not card information, about their clients that is relevant to their program requirements.

Within the IAS, the information model is further decomposed into information domains, as shown in the following diagram.

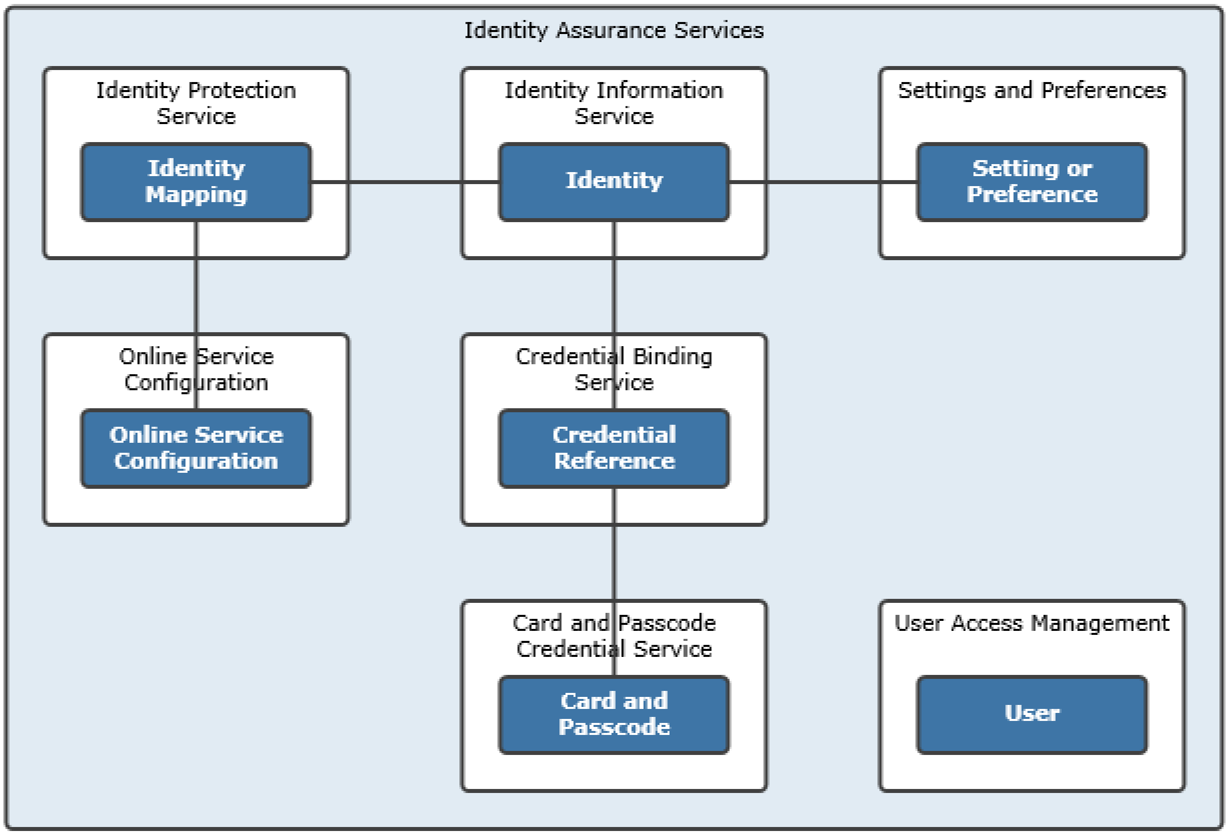

Identity Assurance Services
Identity Protection Service
Identity Mapping
Identity Information Service
Identity
Settings and Preferences
Setting or Preference
Online Service Configuration
Online Service Configuration
Credential Binding Service
Credential Reference
Card and Passcode Credential Service
Card and Passcode
User Access Management
User

Figure 18: IAS Conceptual Information Model

Each registered identity in the IAS is associated with one or more cards and their corresponding passcodes. This relationship occurs with a credential mapping to allow for the representation that the physical plastic card can change over time, but the association of an identity and the current card itself remains constant.

Each registered identity in the IAS has a unique and distinct identifier for each external system that the identity is associated with. During the card issuance business scenario, identifiers are established for identities in ICBC, IAS and Health. During the card authentication business scenario, identifiers are established for identities in online services. The IAS stores the identity mappings for each online service.

An identity or a card may be associated with an individual's preferences that specify how the individual set up their BC Services Card account.

3.3. Technology Architecture

The technology architecture of the Identity Assurance Services is described in terms of an overview of the technology stack. The IAS system components are implemented using several off-the-shelf products and existing standard government infrastructure services.

- The collection of IAS applications and services is custom-developed software implemented on the SoftwareAG webMethods middleware platform.
- The IAS databases are implemented on the Oracle Database Enterprise Edition with DataGuard and Advanced Security functionality.
- User authentication services for government workers are implemented with government's Corporate Authentication Services.
- The SoftwareAG webMethods middleware platform and Oracle Database software are hosted by HPAS as part of government's managed hosting service.

The technology architecture supports the IAS application and data architectures of multiple layers:

- Applications – software functionality that has a user interface, implemented as Java web or mobile applications or portlets within webMethods;
- Integration – software functionality that provides technical capability for the IAS to interface with external systems using file-based, web services and SAML approaches;
- Services – software that exposes, secures and executes business logic and retrieve and update data in the IAS; and,
- Data – software that supports the storage and retrieval of information in a database.

3.4. Security Architecture

The security architecture of the Identity Assurance Services is described as a summary of the security controls applied to the IDIM program and the information, application and infrastructure which comprises the IAS.

Governance, Policy and Standards

IM/IT governance within government flows from the Core Policy Chapter 12 to the operational policy manuals including the Information Security Policy, the Freedom of Information and Protection of Privacy Manual, and the Recorded Information Management Manual. The IM/IT Standards Manual also supplements the Core Policy Chapter 12 and the above operational policy manuals with the detailed definition of information management, architecture, security and privacy controls.

Protection of Information in Transit and at Rest

Information exchange occurs between systems or organizations during card issuance and management processing, online and in-person authentication processing and as part of general IAS data processing and backups. As part of these processes, information is stored secure databases, and in some cases in temporary files. This information is handled in accordance with government standards and information security policy.

Authentication and Access Control

IAS applications follow government standards and information security policy for authentication and access control. Government worker user accounts (IDIR) and the Corporate Authentication Service (including SiteMinder) are used for authentication and access control where the technology products support them. User account password validity periods and application session lifetimes are set in accordance with information security policy.

Access to the IAS applications and systems is role based where supported; access is denied by default and granted on a need-to-know, least privilege basis.

Logging and Monitoring

To satisfy Information Security Policy requirements, the IAS logs activity in the system to support access control monitoring and possible security incident investigations.

Systems are monitored to detect insider abuse and inappropriate access or modification of data. Individuals may monitor their personal card usage in the Account application.

A Security Information and Event Management (SIEM) solution is in place to centralize and secure infrastructure audit and log files to support security investigations and enable automated alerting.

Also, an Operational Records Classification System (ORCS) schedule has been established to define retention, archive and destruction for log and audit information specific to the BC Services Card program.

Data Backup & Recovery

IAS software, database content, application code, operating systems and associated logs are backed up using the government's standard backup service. Backups are performed in a manner that does not affect system availability and are stored and maintained in a manner that adheres to information security policy.

Recovery procedures are established by the production operations team. When required, recovery procedures are initiated by system administrators and performed only against the device from which the backup was taken.

Network Topology

IAS servers are located in network zones that are appropriate for a) the data that is being stored and b) the access that is required. The IAS database servers are located in the Restricted High Security Zone. Application and web servers are located in the High Security Zone.

Servers are grouped into logical network segments based on the host environment in which they provide services (Development, Test, Production). Administrative access to servers is facilitated by access gateways or secured network connections. Internal user access is controlled by public network facing proxy servers. Access to external systems (ICBC, SecureKey and Health Client Registry) is accomplished using secured network connections or public facing proxy servers. Communication with online services occurs using secured network connections between the user's browser and IAS, and between the IAS and the online service.

Availability

The primary goal of the IAS is to securely store and manage information to support card issuance and provide functionality to enable delivery of services to individuals by government programs. In order to provide quality services, the IAS system is designed to achieve a 99.7% up-time rating.

Physical Security

Physical and environmental security of the government's data centers and their associated staff is provided by HPAS as part of government's managed hosting service and meets all government IM/IT standards and information security policy.

The IDIM program work environment is controlled using photo identification and building access cards which are used to positively identify staff and control access to areas of the workplace. Within the work environment, program staff are required to and trained to follow government security controls to manage and protect electronic and paper records.

Change Management

All IAS server hardware and their associated operating systems are managed by HPAS as part of a government's managed service using processes defined by the Office of the CIO. The IAS application, network, database and other software configurations are governed by program specific management procedures.

Incident Management

IDIM's internal incident management uses a combination of existing call centers/procedures and tools to manage questions, information incidents, security breaches and other related events. IAS-specific procedures have been implemented where required.

Testing

A wide variety of testing activities were conducted during the IAS development projects to ensure that the system is both functional and properly secured. From a security perspective, this includes testing that the physical infrastructure has been appropriately hardened against intrusion, that the IAS application code adheres to secure coding practices and does not expose security vulnerabilities, and also includes testing that IDIM program staff are able to respond to an information incident.

Security Management

Informational education material has been developed to assist individuals and IDIM staff in understanding their responsibilities in ensuring a secure online experience. IDIM program staff also work to ensure that BC Services Card services are secure and not being replicated by unauthorized third parties.

Partner Management

A registry of external systems, suppliers and partners is maintained as part of service management activities.

Software Development Lifecycle

IAS is developed using an Agile methodology in which system components are designed, built and tested in small increments spanning short timeframes. Multiple increments are required to produce a finished system.

Security Assurance

A security assurance practice has been established to ensure management of the security aspects of the IDIM program and the IAS system on an ongoing basis, including internal and external testing and ensuring that critical job roles are filled with appropriately qualified staff.