TRIDENT™

TRusted IDENTity

Business Guide

December 2nd, 2022

Table of **Contents**

TRIDENT™

TRusted IDENTity

Introducing Trident

Trident is the name for a range of offerings from the Government of Barbados related to identity management and authorization. It stands for Trusted Identity. The first component to be introduced is the new Trident Identity card which is explained in this document. In the future, there will also be a mobile application which will link with your Trident card to allow you to prove your identity and confirm transactions electronically from anywhere at any time.

Intended Audience

This document is intended for the agencies, organizations, institutions and businesses which wish to interact with the Trident Card. It makes the assumption that the information in the User Guide has already been reviewed and builds on this information by providing more detail on business cases and high-level technical information. There is an additional technical guide which details interactions at a API and card interface level.

For more information please contact the Ministry of Industry, Innovation, Science and Technology at 535-1200, the Electoral and Boundaries Commission at 535-4800 or email info@trident.gov.bb.

Access Modes & Security

In all cases it is assumed that the holder of the card carries a level of responsibility for the safe care and protection of the physical card. Further, for functions that require a PIN number, it is the user's responsibility to keep this number secret. Sharing a PIN number means that a person now has knowledge that enables them to perform actions without your further consent, and there is nothing to stop this individual from sharing your PIN number with others.

The card has a number of access modes each of which have a different level of security. In choosing which functions to use the service provider must consider the security requirements and implications of a given access mode.

Unprivileged vs Privileged

The card allows for different levels of information access based on specific needs for information. An Unprivileged user is an unknown user who has access to the most limited dataset, this is generally limited to the information that could have been physically read off of the card or any service for which it is a proxy document. A Privileged user is one who is known and registered with the authority from which the data is being requested and has demonstrated either a legal right to information, or warrants that a user has given permission for the information to be accessed. Cases of significant volumes of Unprivileged requests may be monitored and such users advised that they should transition to a Privileged status to allow for more complete query logging.

Query Logging

All electronic requests for information must be logged and these logs must be made available to the user on request. Queries from Unprivileged users will be limited to basic information, such as, time of request and IP address of the request since no other information will be available. Requests from Privileged users however will contain details including the name of the individual or the entity requesting the information, the date and time of the request and the data requested.

Visual

The most basic access mode is visual. The RP (Requesting Party) can then manually copy information from the card, take a photo or photocopy of the card for records and otherwise access and store the information that is printed on the front of the card.

Consent

The holder provides consent by handing or showing the card to the service provider.

Validation

The RP is responsible for using the visual security features to validate the authenticity of the card.

Information Security

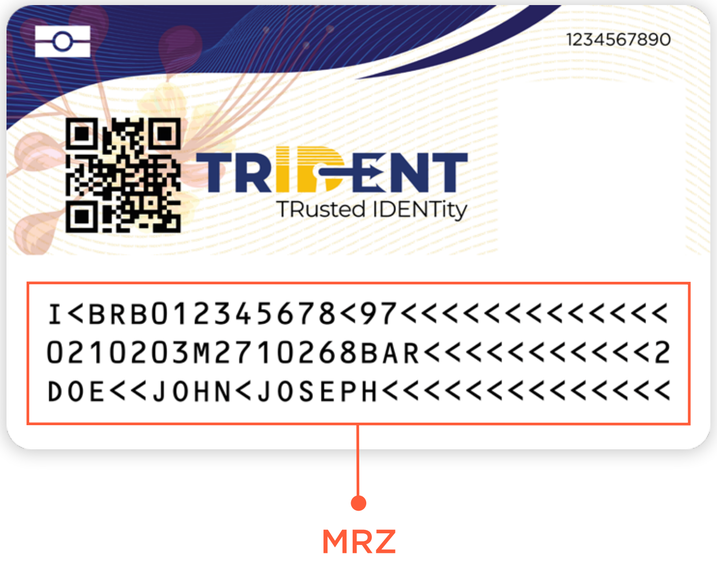
None. Anyone with access to the card can reasonably read or copy the information printed on the card.

Logging

Since there is no way to track visual presentation of the card, no logging is possible.

Usage Example

All current uses of the Barbados ID card.



Machine Readable Zone

The Machine Readable Zone or MRZ provides the information on the front of the card in a format that can be read using optical character recognition. It allows for the fast creation of documents by providing the following information

- Type of Document
- Issuing Country
- Document Number
- Barbados ID Number
- First Name
- Last Name
- Date Of Birth
- Sex
- Date of Expiry
- Nationality

*Continued on the next page

Machine Readable Zone (Cont'd)

Consent

The holder provides consent by handing or showing the card to the service provider.

Validation

The MRZ does not provide any authentication of the document. It is up to the RP to confirm that the person presenting the card matches the person to whom the card was issued. The RP is responsible for using the visual security features to validate the authenticity of the card.

Information Security

None. Anyone with access to the card can reasonably read or copy the information printed on the card.

Logging

Since the MRZ is an optical read and therefore visual, there is no way to track presentation of the card and no logging is possible.

Usage Example

Entry in to a building where it is required to fill in a log book. Scanning of the MRZ and visual verification by security means accurate record keeping, faster processing and zero or minimal contact.

Quick Read Code

The QRC provides a validator to confirm that the card was issued to a particular individual. If scanned by a normal phone, it returns a URL which can be opened in a web browser. It displays the same basic information that is printed on the front of the card. It can be used by the Government of Barbados to provide access to additional information and the first use-case for this is the provision of Driver's License information

The validation process from the QR code can be used by 3rd parties to develop their own solutions which validate the card presented.

*Continued on the next page

Quick Read Code (QRC) (Cont'd)

Consent

The holder provides consent by handing or showing the card to the service provider.

Validation

The QRC uses the signed string in the URL to verify that this card was indeed issued by EBC and that the card is assumed to be genuine for most basic transactions. It is up to the RP to confirm that the person presenting the card matches the person to whom the card was issued. The RP is responsible for using the visual security features to validate the authenticity of the card.

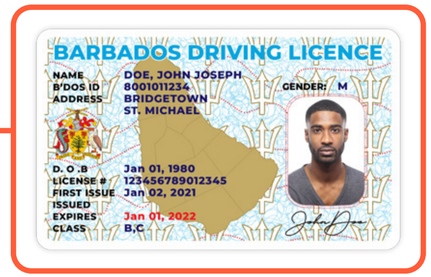
Information Security

Basic. Anyone with access to the card and to a smart phone can reasonably retrieve and read or copy the information which is the same as printed on the card, however the QR Code is electronically validated prior to providing information which confirms:

- That this QR code was issued to a card belonging to the named individual.
- That this card is currently active and has not been reported as lost or stolen.

*Continued on the next page

Quick Read Code (QRC) (Cont'd)



Usage Example 1

Used to provide access to real-time driver's license information. Scanning the card with a mobile device returns the most current information from the Barbados Licensing Authority's database. The ID card is not a replacement for a driver's license but allows information that is outside of the card to be accessed.

Usage Example 2

Purchase of Alcohol/Tobacco products. A merchant can develop a hardware/software solution where the QR code can be scanned and simply have a red or green light indicating if the customer is above the age required. This system would parse the URL from the QRC, execute an independent query to EBC to validate the QR code and request only the age of the holder. Such requests for information would be governed by the Data Protection Act and the EBC's operating guidelines.

Logging

A QRC read by an Unprivileged user will be logged with the date/time and IP address of the request. A QRC read by a Privileged user will include the name of the requestor and the information requested. Information available via the QRC is limited to information that could otherwise be visually obtained from the card or drivers license.

Near Field Communications (NFC)

The card contains a hybrid chipset and antenna which allows access to information on the card through NFC. Different zones of the card have different access conditions and some of these are enabled for NFC. Since the two types of zones that are accessible via NFC have different security and usage profiles they are separated below.

1 Public Zone

This area contains two data fields

- The card serial number
- A signed string similar to the QR code which can be used to validate the card. Available only to privileged RPs.

Consent

The holder provides consent by handing the card to the service provider or by tapping it on a reader.

*Continued on the next page

Near Field Communications (NFC) (Cont'd)

Validation

NFC validation uses the same signed string method as the QR code and therefore acts as a basic confirmation that the card was issued by the EBC. It is up to the RP to confirm that the person presenting the card matches the person to whom the card was issued. The RP is responsible for using the visual security features to validate the authenticity of the card.

Information Security

The Public Zone is secured by keys as are all other zones, however the keys for this zone will be distributed to registered developers rather than be specific to a single developer. It is important to note that the range of NFC is usually less than 2-3 inches however there could be bad-actor scenarios where NFC is read from within a person's pocket or wallet. Therefore the information that is obtainable via the public zone on NFC should never be used for any service other than account linking and identity should be otherwise verified.

Should the key be leaked or too widely circulated, The elements in the public zone of the NFC could be copied and reproduced and therefore, assuming this risk, the public zone should only be used in low-risk situations and in combination with other forms of verification.

*Continued on the next page

Near Field Communications (NFC) (Cont'd)

Logging

As reads of the NFC Public Zone are completely within the card itself, there is no ability to log the reading of data. However, information request for data on the basis of the information on the card will be logged. If the resulting information is used or processed in any way, the provisions of the Data Protection Act must be adhered to.

Usage

As a replacement for the standard loyalty card, an RP can link the holder's information with their rewards account and thereby allow them to use their ID card instead of an issued loyalty card. This allows simpler entry in to loyalty programmes, less operational overhead and added convenience to the holder – one card for all uses.

*Continued on the next page

Near Field Communications (NFC) (Cont'd)

2 Secured Zone

The NFC also allows access to a limited number of separate secure zones that can be used for a number of purposes. These zones can have separate read and write keys which means that reading from these zones is limited to entities which have access to the keys and that writing privileges can also be separated. Therefore a given RP may have the ability only to read secured data from this zone or to both read and write data to this zone, for example for use as a bus pass.

Consent

The holder provides consent by handing the card to the service provider or by tapping it on a reader.

Validation

Information in the public zone is used, along with other information to generate the specific keys for this particular card and this particular session. Therefore the ability to access the information with the correct keys implies validity of the card itself. It is up to the RP to confirm that the person presenting the card matches the person to whom the card was issued. The RP is responsible for using the visual security features to validate the authenticity of the card.

*Continued on the next page

Near Field Communications (NFC) (Cont'd)

Information Security

High. The information storage area is protected by keys which are unique to each card. Therefore access to the information in these zones is reasonably secure. Information within these zones can also be encrypted to provide further security if required.

Logging

NFC reads of on-card information are not logged since there is no record of the transaction, however if the resulting information is used or processed in any way, the provisions of the Data Protection Act must be adhered to.

Usage

As a transportation pass, this area can be used so that only the provider can read and write information to this area of the card. While the transportation solution is understood to be an online system where transactions against a mobile wallet are processed immediately, there may be circumstances where internet access is not available. This system allows to provider to read previous balance information and write transaction information to the card in such circumstances and to be reconciled when connectivity is restored.

It is important to note that the card should never be used as a store of wealth. Transaction registers such as this should only be used as a backup to a primary system.

ICAO MRTD

The card is an ICAO compliant travel document. The process for reading Machine Readable Travel Documents (MRTDs) involves the use of both the MRZ and the NFC components and uses a separate application on the card, eTravel, for this purpose. The process is as follows:

1. The MRZ is read and from this is extracted a key to unlock the eTravel application over NFC.
2. The eTravel application returns the information to the requestor. This information includes the same information on the front of the card as well as:
   - Country of birth
   - Eye colour
   - Distinguishing marks
   - Passport photo
   - Hair colour

*Continued on the next page

ICAO MRTD (Cont'd)

Consent

The holder provides consent by handing the card to the service provider or by inserting or placing it on a reader.

Validation

Validation is done in accordance with ICAO 9303 as to the validity of the signer of the document.

Information Security

Security is in accordance with ICAO 9303 BAC.

Logging

The process of reading ICAO compliant information from the card takes place entirely on the card and therefore it is not possible to log. However if the resulting information is used or processed in any way, the provisions of the Data Protection Act must be adhered to. In cases where the information from the eTravel application is used as part of a KYC process and additional information is required from EBC to validate, this complete transaction would be logged and must be performed by a Privileged user.

Usage

This mode of access allows for the card to be used as a travel document subject to international agreements. As the information returned includes the photo of the user, it allows for KYC and remote onboarding applications using facial recognition technologies. A live user can be compared to the stored photo for verification. The document number can further be validated with EBC to ensure card validity. This mean that this mode of access has a wide range of potential use cases including in-person and remote identity verification. In cases where the user has given additional explicit consent, verified address information may also be obtained from EBC to complete the KYC process.

Cost

There will be a nominal cost for KYC queries against the EBC database. This is to support the activities required to ensure the accuracy of the information provided. We are working with a small pool of stakeholders to test this functionality and also to determine reasonable pricing.

Chip (Contact) Interface

As with NFC, there are additional zones on the card which can only be read when the card is inserted into a reader.

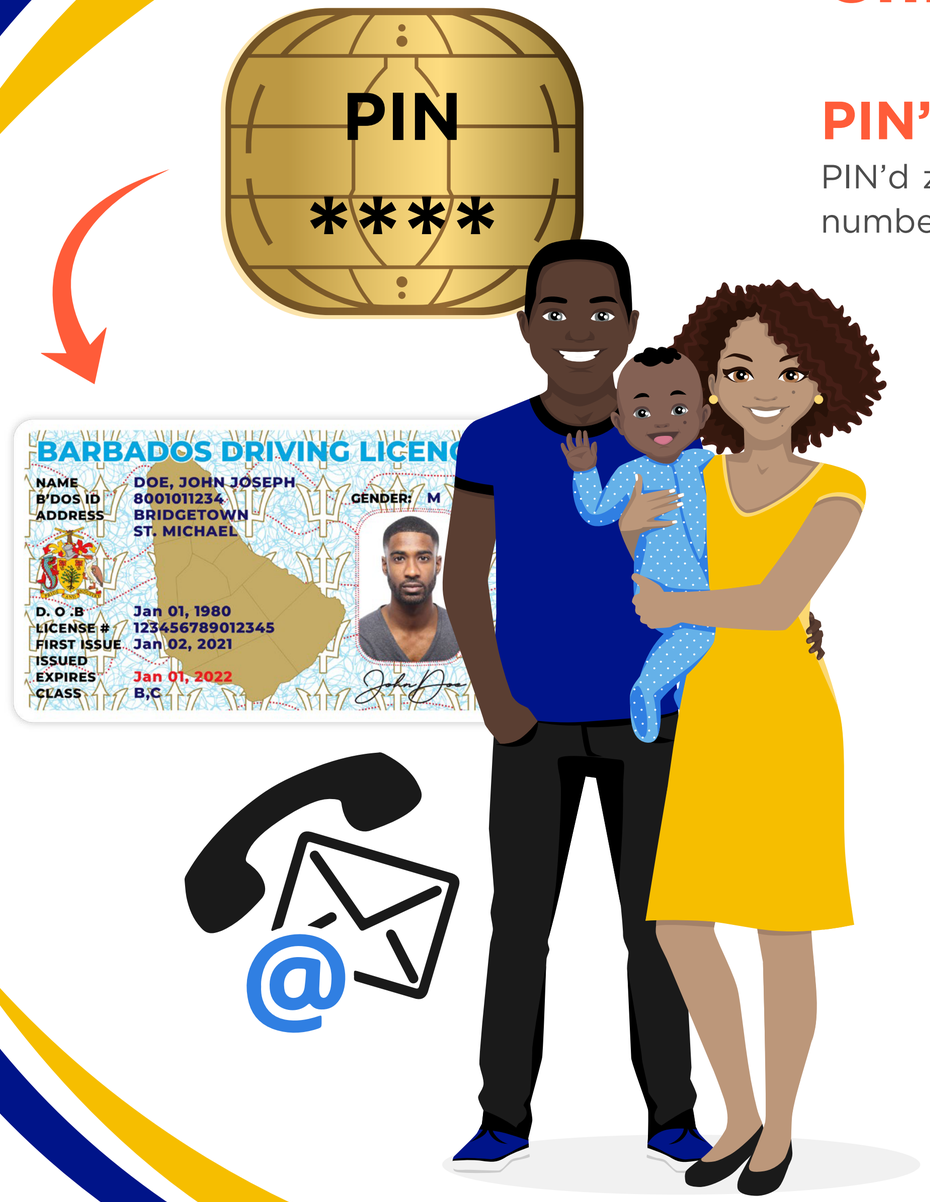
Since the two types of zones that are accessible via the Contact Interface have different security and CI usage profiles they are separated below.

Private Zones (Keyed and PIN'd)

There are two types of private zones when using CI. Firstly keyed zones which are otherwise identical to the private zones discussed under NFC with the exception that they required the card to be physically inserted. Secondly zones that are secure by a PIN number.

*Continued on the next page

Chip (Contact) Interface (Cont'd)



PIN'd Zones

PIN'd zones require the holder to unlock by entering a key (4-digit PIN number). There are two zones which currently support this functionality:

EBC Data

This is an expanded dataset of information from the EBC database including address and contact information, immigration status and category. In the case of cards issued to minors, this area also includes information on primary and secondary guardians.

Driver's License Data

While it is intended that in most use cases driver's license data will be provided in real-time from the BLA database, there are circumstances where access to DL information may be needed in an offline environment. An expanded set of DL information is stored in this zone. This zone also has a separate read-only key which has been provisioned but not currently in use and this has been done to support future developments. The data structure is compliant with ISO 18013-2 however the card itself is not.

*Continued on the next page

Chip (Contact) Interface (Cont'd)

Consent

The holder provides consent by tapping or inserting the card into a terminal and entering a PIN number known only to them. This achieves the highest level of consent using a minimum of two factors of authentication.

Validation

Validation of the PIN number is done on card and verifies that the user knowns the PIN. It is up to the RP to confirm that the person presenting the card matches the person to whom the card was issued.

*Continued on the next page

Chip (Contact) Interface (Cont'd)

Information Security

High. The information storage area is protected by keys which are unique to each card. Therefore access to the information in these zones is reasonably secure. Information within these zones can also be encrypted to provide further security if required. For transactions which involve a PIN, unless the user has allowed their PIN number to be compromised, there is the highest level of assurance that permission has been received for any sharing of information.

Logging

In all cases where a request takes place entirely on the card there is no ability to log the request. However if the resulting information is used or processed in any way, the provisions of the Data Protection Act must be adhered to. For PIN-based transactions, the Privileged user is required to keep logs of all transactions.

How can I find out more?

For further information you may call **536-2343**
or email us at **support@trident.gov.bb**


TRIDENT™
TRusted IDENTity