

White Paper:

Delivering Secure End-to-end Solution for e-Passport Programmes



International e-Passport initiatives are utilising advancements in biometrics and contactless smartcards, as the key technologies driving the enhanced traveller verification programmes, providing means for more effective and efficient border controls, safer air travel and, ultimately, stronger national and international security.

MULTOS, as a highly secure, open, multi-application smartcard environment is particularly suited for security critical projects such as e-Passport deployments, where trustworthiness, integrity and authenticity of a document and the privacy of person's data are of utmost importance.

Objective

The complex matrix of business requirements for an end-to-end e-Passport solution has to address: adherence to the relevant ICAO technical recommendations, security level of the chosen e-Passport contactless platform, flexibility and robustness of the supply chain, existence of tools and supporting infrastructure to ease the deployment and integration with the existing systems and processes.

The intention of this White Paper is to address some of technical, security and business issues associated with the use of chips and biometrics on passports, and to discuss benefits of employing MULTOS based end-to-end solution in the context of an e-Passport project environment.

Benefits of Open Platform v. Native Implementations

Robust Supply Chain

Long term, large scale projects such as national e-Passport deployments, require solutions that are based on open standards. The result is - a robust supply chain, where each component of the system is interchangeable and can be sourced from multiple vendors rather than relying on solutions provided by a single source as is often the case with native platforms.

One of key business propositions for MULTOS is the capacity to provide issuers with choices right across the supply chain - from multiple silicon suppliers, MULTOS implementations, personalisation system vendors, e-passport management systems providers and independent application development sources.

This is achieved by strict adherence to MULTOS open specifications, common Security Target, and mandatory, independent third party Type Approval process. All are required to guarantee full cross-platform interoperability and backward compatibility at all levels of the supply chain. Other open platform solutions based on competitive technologies, usually do not employ full Type Approval process, and have, today, a difficulty in ensuring interoperability across all platforms.

MULTOS is also a mature and proven technology, with a base of over 30 million smartcards issued worldwide in various security sensitive projects across Banking and ID markets. It is already well supported by the industry leading vendors, with off-the-shelf products, providing e-Passport issuers with additional confidence in the longevity of the MULTOS scheme and, consequently, lower risk.

Simplified Upgrades

The standardisation work on travel related documents and services is far from finished. For example, features such as Extended Access Control which have not (yet) been specified in current ICAO recommendations, are being discussed as part of European initiative to further protect more sensitive e-Passport data such as fingerprints or other supplementary biometrics.

In this dynamic environment, when specifications are still being decided on, chosen e-Passport platform has to provide means for easy addition of any new feature that might become required as the work on electronic MRTD standards progresses.

Unlike native platforms, which usually are designed so that the application functionality is hard coded in ROM area, Keycorp e-Passport solution is architected around MULTOS secure operating system, which allows ICAO application to be securely upgraded or modified, without making the existing, un-personalised e-passport base obsolete.

Multi-application platform in the context of e-Passport

Does e-Passport need to be based on a multi-application platform?

ICAO specifications are open on this matter. The decision whether to use multi-application platform to allow other travel or a country-specific applications to co-reside on an e-Passport platform is left to the e-Passport issuers and their strategies.

Future-proofing Solution

The standardisation work on e-Visa, for example, is in full swing. Different e-Visa scenarios are being studied, such as:

- whether visa specific data should be included in an e-Passport application, thus making the e-Passport application updateable by the visa-issuing country?
- should e-Visa be specified as an “e-Visa container” application which can be reused for multiple visas? Could this application co-reside on the same contactless chip as the e-Passport application?
- or, should a separate contactless chip be incorporated the e-Passport booklet by the passport issuing country, which would be used solely as “e-Visa container”?
- or is every visa-issuing country going to issue their own contactless e-Visa sticker?

What are the security implications of these scenarios? How many contactless chips can one fit in a passport booklet and expect them to co-work? Many questions are still open.

So, choosing multi-application platform, with high security assurances, provides a future proofed e-MRTD solution.

MULTOS generic and proven, public key based application management protocol provides for that flexibility under full e-Passport Issuer's control:

- It allows secure addition of any new applications to an existing e-passport (potentially applications such as e-Visas)
- it enables secure maintenance of an existing e-Passport application, without the need to

replace the whole non yet issued e-passport base.

In addition to that, e-Passport Issuers may also want to incorporate their own applications on the e-Passport chip, especially for automated border control for their own citizens, at their own borders.

Importance of Security

The ultimate objective of e-Passport initiatives around the world is to create Trusted Travel Document, enabling more efficient and effective control of travellers identity, strengthening border security, while at the same time ensuring that privacy of e-passport holder's data is not compromised.

ICAO recommendations mandate some basic security requirements and provide optional mechanisms for higher security regime that governments can choose to employ in their national e-Passport programmes.

Appendix A of this document deals in more detail with security implications and potential threats associated with the use of chips on passports. It describes some mechanisms that e-Passport application and underlying MULTOS security architecture provide to counter those threats.

No "Back Doors"

MULTOS has been architected from the ground up with security in mind. MULTOS architecture, including on-card operating system as well as the off-card MULTOS card and application management protocols, have achieved the highest level of security evaluation certification today, ITSEC E6 high.

That means that there are no unknown or known "back doors" in the operating system for counterfeiters to exploit. MULTOS security architecture is fully specified. Mandatory security evaluation re-enforces that all MULTOS implementations correctly implement all specified security mechanisms and that no "back doors" or security holes are left open in the platform software.

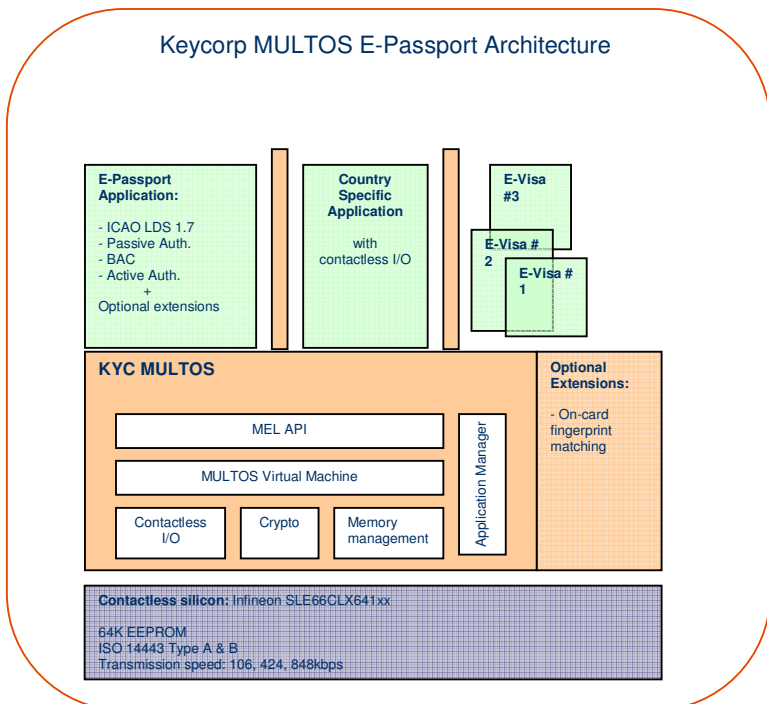
Protection against counterfeiting

Each MULTOS chip is equipped with unique keys, thus ensuring that only

applications authorised by the issuer and targeted for the particular e-Passport chip can be loaded on that individual chip.

As a result, opportunities for counterfeiting e-Passport are significantly minimised:

- Lost or stolen MULTOS chips and / or unpersonalised e-Passports are unusable for counterfeiting purposes. Each MULTOS chip verifies the integrity and source of application and any rogue e-Passport applications, which are not authorised by the issuer are rejected by the MULTOS chip.
- Using stolen personalisation data to modify and produce new passport is impractical. MULTOS personalisation data is encrypted with unique keys, so that it could be decrypted only on a particular target e-Passport chip, which also checks the integrity and source of data. It is impossible to decrypt the file, insert new e-Passport information and then encrypt and sign the new personalisation in such a way that e-Passport chip would not have recognised it.



MULTOS Secure Distributed e-Passport Issuance Model

MULTOS provides an end-to-end security management throughout the entire e-Passport lifecycle.

E-Passport chip initialisation and post issuance management processes are based on the public key architecture, binding the e-passport chip and the e-passport issuer so that only the issuer has full control over the e-Passport chip and all its contents.

This unique capability enables a secure and scaleable distributed e-Passport issuance. In this model, blank MULTOS e-Passports can be safely distributed to the embassies and consulates around the world, to be personalised locally, at the time a new or replacement passport is being requested.

Choosing MULTOS for e-Passports could also significantly reduce investment and time to full deployment, since many established processes and existing infrastructure used in numerous MULTOS smartcard programmes around the world could be reused.

The following is description of how this might work. For convenience we have considered this in two stages, the first being the e-Passport Assembly, and the second being the e-Passport Issuance process. The processes are shown graphically in the diagram below.

MULTOS e-Passport Assembly

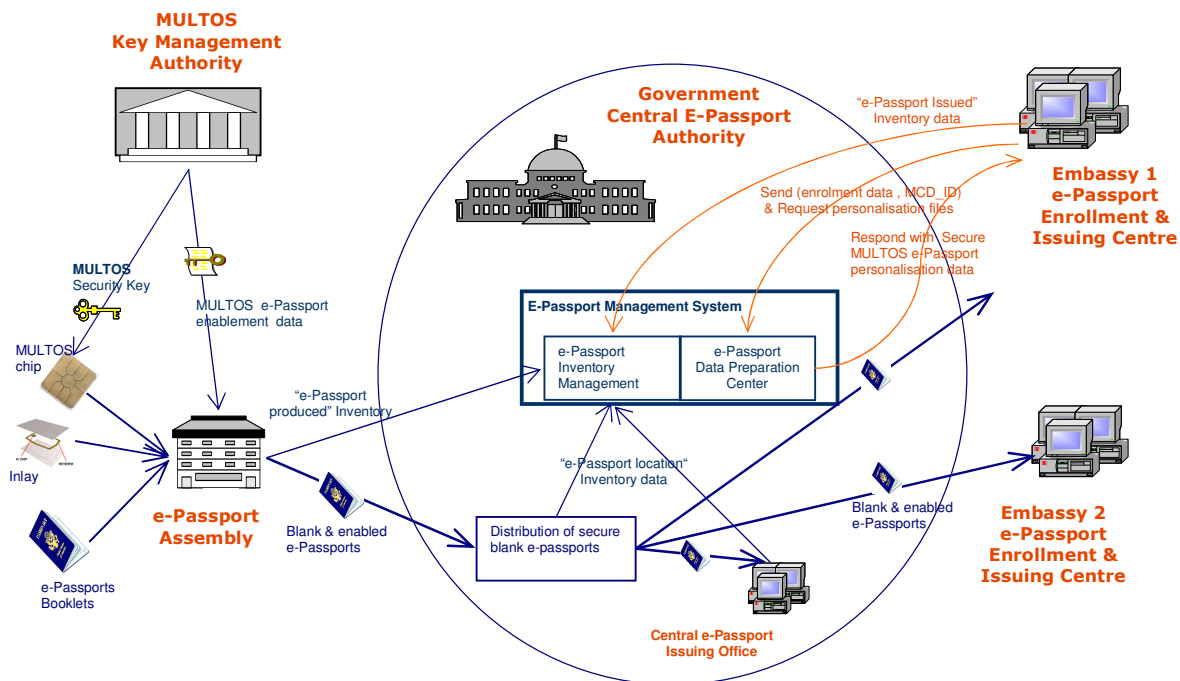
The sequence of steps in the manufacturing process may vary in practise, but it can be assumed that MULTOS contactless modules and aerials will be assembled and united with traditional blank passport materials to create a blank e-passport document.

At that stage MULTOS chip id (MCD_ID) can be read and used as the identifier of each e-Passport document. The MCD_ID can be sent to the existing MULTOS Key Management Authority (MULTOS KMA) to generate enablement data for each MULTOS e-Passport.

The MULTOS MCD_ID can be sent to the e-Passport Management System (a derivative of a Card Management Systems), where it could also register the location of the e-Passport to be at the production centre.

As e-Passports are required to be shipped to issuing centres (especially if they are shipped overseas), the MULTOS MCD_ID can be read, and the e-Passport identified as being shipped to a different location. This history can be retained on the e-Passport Management System.

Blank e-Passports can then be held in issuing locations where they will be used.



MULTOS E-Passport Issuance

It is assumed that e-Passports will be issued both in the country, and in some of the country's overseas diplomatic representations. Each Issuance Centre will have to be equipped with enrolment systems able to capture personal data and biometric images.

At the enrolment stage, the enrolling officer will select the blank MULTOS e-Passport that is to be issued for the particular candidate and the MULTOS chip MCD_ID and public keys will be read, and sent electronically to the Central E-Passport Data Preparation Centre, together with the enrolment details.

At the Central e-Passport Data Preparation Centre, the enrolment data and MULTOS MCD_ID will be used to create a MULTOS ICAO Application Load Unit (ALU) containing personalisation data that will be used for this e-Passport, which will include generating unique e-Passport keys and signing the data using the Governments Private Keys.

The MULTOS ALU will then be encrypted using the chip's public RSA key. E-Passport Management System will be updated with the e-Passports encrypted ICAO ALU details as well as any other applications that the Government may wish to include on the chip.

The e-Passport Management System can then send the encrypted MULTOS ICAO ALU to the location where it understands the e-Passport to be resident. The encrypted ALU can only be decrypted within the targeted chip so that transmission can take place over the public IP network with no risk and without any additional security infra-structure having to be built.

At the issuing location the blank MULTOS e-Passport can be presented to a Issuance workstation and the MULTOS ICAO ALU will be loaded to the e-Passport chip and subsequently decrypted within the chip.

To print the details page of the e-Passport, the e-Passport chip can be interrogated and the details to be printed can be extracted, formatted locally and printed before the e-Passport is finally sealed.

After the Passport holder has collected the e-Passport, a message can be sent to the e-Passport Management System to indicate the e-Passport has now been issued.

E-Passports reported lost and stolen should also be recorded in the e-Passport Management System so that a complete inventory record can be retained.

E-Passport Performance

To maintain worldwide interoperability of biometric passports, ICAO mandates that each biometric type is stored as a complete image, while the storage of templates is optional. That way, the image can be used at all border control inspection systems which will more than likely be equipped with biometric recognition systems provided by different vendors using vendor specific biometric recognition algorithms.

Achieving interoperability at this level, pays the price in the size of data that has to be stored in the e-Passport chip.

ICAO studies have shown that an optimum size for an e-Passport facial image compressed using JPEG and JPEG2000 techniques is between 12 - 20KB without downgrading its potential for recognition. Similarly the optimum size of a fingerprint image has been found to be 10KB per each finger, while an iris image is estimated to take approximately 30KB.

The more data is stored in the chip, the longer it takes to read out at the border control points.

Target Data Retrieval times are provided in the ICAO recommendations for inspection systems and e-Passport solutions to aim for:

ICAO Recommendations:	
Size of data (assuming only Passive Authentication is configured and no other security options are enabled)	Target retrieval time (s)
~ 15Kbytes	<1.25s
~ 30Kbytes	<2.50s
~ 64Kbytes	<5.00s

However, at the recent ICAO interoperability tests, measured data retrieval times were often outside targeted values expected in the ICAO document. The performance measurements captured at ICAO interoperability tests in Tsukuba, Japan, in March2005 were:

Test Results 1:

Essen Group - Preliminary Test Results – average data retrieval time		
Size	Without BAC	With BAC
~ 20K (standard ICAO data set)	4.6s (min 2.2s)	11.6s (min 3.0s)

Test Results 2:

Tsukuba – Preliminary Test Results (20Kbyte with BAC)			
Reader	average	Minimum	Maximum
GRT	5.76s	4.6s	9.4s
NMDA	7.93s	5.6s	11.3s
Other	6.85s	5.4s	10.4s

Keycorp MULTOS e-Passport platform is expected to be at the faster end of that range. The initial measurements carried out using MULTOS development tools, running ISO 14443 Type B protocol, at 424kbps transmission speed, are showing less than 3.0s for 20K of data.

Further MULTOS performance tuning is still in progress. Assuming the readers could also support 848kbps transmission speed, as desired by ICAO, the throughput would be further improved.

MULTOS true end-to-end security architecture delivers efficient and cost effective solution for e-Passport programmes.

Appendix A: Security and ICAO standards for e-MRTDs

Introduction

This document is intended to review some of the security implications and potential threats associated with the use of contactless chips on e-Passports within the context of the new ICAO recommendations for Machine Readable Travel Documents (MRTDs).

ICAO provide basic recommendations for security and provide an optional regime for higher security. The mandatory requirements are:-

- The IC/Operating System SHALL provide means against unauthorized writing.
- That each data group SHALL be signed with an RSA key by the Issuing Country so that the integrity can be validated by the 'Inspection System'.
- That the chips used SHOULD have a Security Evaluation to CC EAL4+ against a 'suitable' Protection Profile.

Keycorp believe that further security will be required by most governments and the minimum practical requirement will be implementation of the Basic Access Controls (BAC)¹.

Keycorp note that the ICAO recommendations are still unclear in some areas and work is still ongoing to finalise it. Some of this work will have a bearing on the security.

Keycorp believes that Issuers should be taking at least the following Security Measures into consideration when selecting chips and designing the surrounding infra-structure.

Scope

For the purposes of this document we have considered the following:-

1. The ability to manufacture counterfeit travel documents.
2. The ability to subvert the operation of the chip for illegal activities.
3. The ability to gain unauthorised or inappropriate access to information contained on the chip.

We have assumed that, travel documents are subject to more extreme pressures than the majority of commercial identity documents (bank cards etc) and indeed in addition to normal criminal activity, the resources of government are used by some nations to manufacture travel documents for covert purposes.

We have further assumed that passports will be issued and re-issued from both a central location and from overseas locations (embassies and consulates) for citizens overseas and to deal with lost and stolen passports. With this in mind we have referred to the 'Issuing Office' below as the place where passports are personalised and issued to the passport bearer.

We have only given consideration to the 'Chip' within the MRTD.

Damaged Chips

A traveller, using a counterfeit passport could present the MRTD with the chip apparently or actually damaged and non functional and may be able to use such a passport for some time.

Inspection Stations will have to have procedures to deal with documents that have inoperative chips.

We are presuming that some protocol between nations will rapidly come into operation for advising of passports with damaged chips to meet with obvious threat and note that this is a universal problem and outside the scope of this paper.

In the scenarios below, the damaged chip issues are mention in this context. We assume though, that for any holder of an illegally manufactured or modified passport would wish to attract as little attention as possible and would therefore wish to have an operational chip within the passport.

Passport Issuing Operations

If travel documents become more difficult to manufacture illegally, pressure may be brought to bear on the next most vulnerable point which could be the issuing and enrolling process. Issuing authorities will have to ensure that security measures and checks are in place to ensure that corruption of these operations does not occur instead of passport counterfeiting.

¹ See 'Technical Report, PKI for Machine Readable Travel Documents offering ICC Read-Only Access' version 1.1 1/10/2004.

Miss-use of Validly Issued Documents

One scenario that is used by illegal travellers is to acquire a passport where the picture is similar to that of the illegal traveller and as application change the appearance of the traveller to suit the image on the passport. This threat is not dealt with by the ICAO standard unless the use of fingerprints is invoked, and this will only be effective if the chip is not damaged.

Chip Threat Analysis

Lost and Stolen Chips.

Lost or stolen chips that have not been integrated into passport bodies (without the proper security measures) could be used in the fabrication of counterfeit passports.

Basic minimum measures need to take place to ensure that chips are protected and accounted for during manufacture, delivery and storage. Further, chips if lost or stolen, should not be useable for the creation of counterfeit passports.

MULTOS provides this protection because the chips are not useable by anyone until they are enabled, and can only be enabled by the Government using data which is generated by the secure MULTOS KMA.

Lost and Stolen Passport Bodies (pre-chip)

Lost and Stolen passport bodies before the chips have been integrated could be used in the fabrication of counterfeit passports, and cheap common available chips could be added to provide the machine readable functionality.

The ICAO recommendations require the Data to be signed by Keys unique to the Government provides some protection against this.

Damaged and inoperable chip scenarios are also applicable here.

It cannot be assumed that the insertion of the chip in the Passport makes the document more secure or the passport body less valuable than is currently the case.

Lost and Stolen Completed Passport Bodies (Chip Included)

These too are obviously an aid to counterfeiters, however, applications and data will still have to be loaded onto the chip.

Our recommendation is that, applications and Data are loaded using the MULTOS load and delete mechanisms so that applications are signed and

encrypted in the secure facilities of the Central e-Passport Data Preparation Centre and then transmitted to the Issuing Office where they can be loaded onto chip and decrypted within the chip. This prevents anyone being able to add or delete applications, keys and/or data from the chip.

The e-Passport Management System (a derivative of existing Card Management Systems) can be adapted to track the location and status of all chips and passports from the time that the IDs of the chips are first presented to the system.

Damaged and inoperable chip scenarios are also applicable here.

Lost and Stolen – Issued Passports

Traditionally lost and stolen passports have been used to modify as applicable to create false identity.

With the new system illegal use of Lost and Stolen passports will become somewhat more difficult because the chip data will need to be modified as well (see below for further details).

Damaged and inoperable chip scenarios are also applicable here.

Modification of Data on the Chip

The ICAO specification mandates that the data shall not be capable of being modified by unauthorized persons. This would normally mean that the application had to have some means (perhaps password) for identifying the authorized person before the data could be modified. Keycorp notes that such passwords can be vulnerable depending on how the application is designed and would recommend that the application be developed without any means writing to its files (that is, the application is designed to be read-only) and that Data be loaded as part of the process for loading the application to the chip using the MULTOS secure application load methodologies. This would also protect the data from being modified during transmission and loading the data.

All the data carried on the chip in the ICAO designated 'Data Groups' is protected by RSA signatures, however Keycorp note that the 'Data Group Presence Map' is not so protected, and further, uses single bits to indicate the presence or otherwise of each Data Group. This means that if the state of a transistor on the chip is changed the presence of a Data Group could be hidden from the Inspection Station. Of these, hiding Data Group 3 (finger prints) and/or Data Group 15 (Document Security Object) especially could have negative impact.

The chips hardware must have the means to hide the location of data so that it cannot be tampered with by electro-mechanical intervention. This is a standard requirement for chips that are used for MULTOS implementations.

The Data within each Data Group is signed by a private key generated by each Issuing Authority. The Security of this key is paramount.

Skimming

Skimming is the ability to read the chips data by placing a reader near the chip and interrogating it using the commands in the ICAO standard, without the knowledge or permission of the Passport Holder. Such data could then be used to make a duplicate chip.

The ICAO standard has provided Basic Access Controls (BAC) to deal with this threat. We envisage that BAC will be a minimum requirement for Governments where personal privacy is likely to be an issue amongst its citizens.

BAC requires the use of DES and RSA cryptography which is supported by MULTOS.

Eavesdropping

Eavesdropping is similar to Skimming above, but requires equipment that can 'listen' to communication between the chip and the Inspection Station. ICAO makes some recommendations to deal with this issue at the Inspection Station but this does not have any bearing on the chip, and cannot be assumed to have been implemented.

Issuers of MRTDs should be aware that this exposure does exist.

Chip Substitution

It is conceivable that a counterfeiter could manufacture a passport and use commercially available memory chips to substitute for chips issued by Issuing Authorities.

The ICAO standard provides an optional challenge and response mechanism to determine whether the chip was issued by the issuing authority. Support of this challenge and response requires 3DES. But note, there is no requirement that the Inspection Station invoke 'Active Authentication' and it therefore cannot be assumed that this substitution will be detected other than by Issuing Governments (who check their own MRTDs according to their own rules.

Attacks on Keys Used in BAC and Active Authentication

Chips can be monitored during use and the patterns of some activities determined which can lead to derivation of keys used for Crypto-graphic purposes. All Cryptographic functions supported on the chip must have defences included so that keys cannot be derived from such monitoring. These operations are standard MULTOS defences.

Perturbation

There are a variety of attacks available that can cause a chip mis-function. Typically these sort of attacks have been used during 'Read' functions in such a way that the information returned is information from some other address in the chips memory, or for instance that the chip continues to read past the ending address of the data that was requested. Attackers can then often determine keys (random binary data) from other more structured data.

Operating systems must be required to support the means to defend against attacks of this nature.

Cryptographic Algorithms

Keycorp notes that the SHA_1 hashing algorithm has been included as one of the optional hashing tools, and further that this has recently been broken. We recommend that the SHA_1 algorithm be not used.

Keycorp Limited

Level 5 Keycorp Tower
799 Pacific Highway Chatswood
NSW 2067 SYDNEY Australia
Tel +61 2 9414 5200 Fax +61 2 9415 1363
Email: info@keycorp.net www.keycorp.net

Keycorp Canada Inc.

Suite 700
3700 Steeles Avenue West
Woodbridge Ontario L4L 8K8 TORONTO Canada
Tel +1 905 265 9196 Fax +1 905 265 2257
www.keycorp.ca