

The IBM Check Point Reader (CP Reader)

Many new identity documents such as driving licenses, passports, residence permits, national identity cards, etc. have an embedded chip capable of storing a digitally authenticated version of the information printed or engraved in the physical document. Moreover, for convenience, security and/or privacy reasons these chips are also capable of storing and protecting information not present in the physical document itself, particularly biometric data such as images of the cardholder's fingerprints or irises.

In order to be able to exploit the full potential of these documents, public and private entities need to be able to read and verify the authenticity and integrity of the information retrieved from these documents' chips. Furthermore, when biometric information, such as fingerprints, is available, it may be useful to be able to validate whether the fingerprints retrieved from the document match those acquired live from the document holder.

The IBM Check Point Reader (CP Reader) accesses data on chips according to the most recent international standards, verifying its integrity and ensuring that it matches the information printed on the card. Once these validations have been completed, it acquires the document holder's fingerprints and performs a comparison with the templates stored in the chip. The result of this process is conveyed to the inspector through a very simple and intuitive user interface, which allows the physical document as well as the information stored in

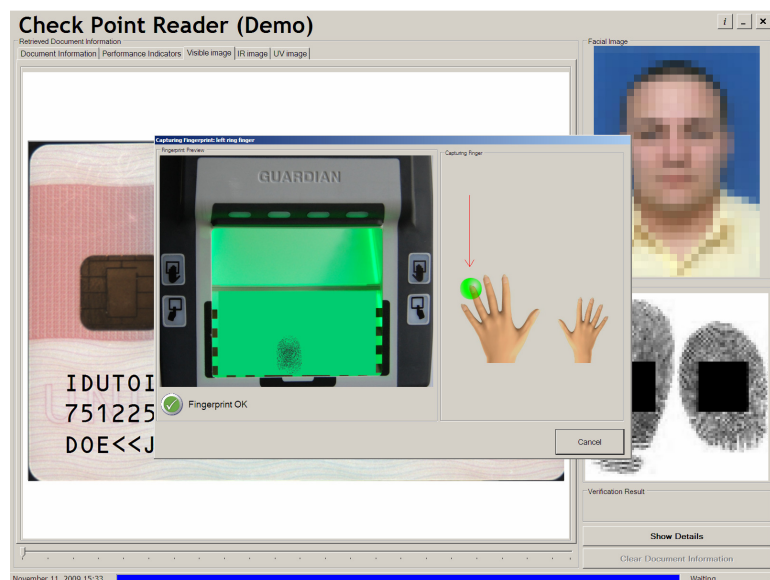
its embedded chip to be further examined.

Basic concept

The IBM CP Reader consists of an application with a simple and intuitive graphical user interface running on a touch-screen kiosk PC. This application has been designed in such a fashion that it demands very little user interaction and training. The document verification process is started automatically once a document is placed on the document scanner, a piece of hardware capable of capturing images from the document, as well as communicating with its embedded chip.

Once the data stored in the document chip has been checked, the document holder is prompted to

engage in a live fingerprint capture, during which one or more fingerprints are acquired using a forensic quality fingerprint scanner. Then, these fingerprints are compared with those stored in the document employing state-of-the-art biometric fingerprint matching algorithms certified by the US government. When the validation process finishes, the inspector is notified of the verification result. If all validations succeed, the information retrieved from the chip can be examined, along with the detailed operation log. Conversely, if any validation fails, a succinct explanation of the failure is given to the inspector, and additional information is provided on lower-level screens so that the root



After validating the integrity of the information stored in the document chip, The IBM Check Point Reader engages in a live fingerprint capture. The fingerprints captured from the document holder are compared to those stored in the document chip, determining whether the document is genuine and it has in fact been issued to the document holder.

cause of the failure can be determined.

In terms of security, the integrity validation trust points, as well as the credentials required to access sensitive information stored in the documents are securely stored in a tamper resistant container which is transparently accessed by the CP Reader and can be managed using the CP Reader ancillary utilities.

Use cases

The CP Reader can be used by immigration authorities to check the validity of domestic and foreign machine readable travel documents. It can also be used in self service kiosks where citizens can check the information stored in their own documents, i.e., to achieve compliance with Freedom of Information Act-like regulations.

Key Features

- Support for **ICAO's Doc 9303** compliant Machine Readable Travel Documents, e.g. passports, visas, and residence permits.
- Support for **Basic Access Control (BAC)**.
- Support for **Extended Access Control (EAC)**.
- Customizable rule sets** depending on the document type.
- Secure storage of credentials** required to access and validate on-chip data.
- Key and Certificate management**, e.g., required for Passive Authentication (Doc 9303) and Terminal Authentication (EAC).
- Simple user interface** designed to minimize inspector interaction.
- Touch sensitive screen** to facilitate inspector interaction and avoid peripheral clutter.
- Portable standalone version available**. All components fit into a briefcase. Ideal for law-enforcement on-spot checks.
- Display of **optical captures from the document** taken under visible, ultraviolet, and infrared light*.
- Display of **photo from chip**.
- Display of **fingerprints from chip**.
- Detailed report of **information retrieved from the chip** available for browsing.
- Detailed report of **validation tasks** executed by the terminal.
- Report of **performance indicators** gathered during the interaction with the document.
- State-of-the-art **biometric fingerprint matching algorithms, certified by the US government**.
- Flexible integration** of additional biometric algorithms and technologies.
- Multiple fingerprint and document scanners** supported.
- Customizable fingerprint gathering policies** (i.e. one or two fingers)
- Customizable fingerprint matching threshold**.

To learn more:
secure-readers@zurich.ibm.com

**The precise amount of captures depends on the capabilities of the Document Scanner.*



Copyright International Business Machines Corporation, 2009
All Rights Reserved.

The following are trademarks or registered trademarks of International Business Machines Corporation in the United States, or other countries, or both: IBM, the IBM Logo, Ready for IBM Technology.

Other company, product and service names may be trademarks or service marks of others.

All information contained in this document is subject to change without notice. The product described in this document is NOT yet generally available via the normal IBM sales channels. The information contained in this document does not affect or change IBM product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of IBM or third parties. All information contained in this document was obtained in specific environments, and is presented as an illustration. The results obtained in other operating environments may vary.

THE INFORMATION CONTAINED IN THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS. In no event will IBM be liable for damages arising directly or indirectly from any use of the information contained in this document.

IBM Research GmbH
Säumerstr. 4
CH-8803 Rüschlikon
Switzerland

The IBM Zurich Research GmbH home page can be found at <http://www.zurich.ibm.com>.

The IBM home page can be found at <http://www.ibm.com>