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.

A key part of any personalization system for these documents is quality control: checks to ensure that the cards and chips have been personalized correctly. While data printed on the card can be verified by optical or manual inspection, data stored on the chips needs to be read and verified electronically. The IBM Quality Assurance Reader (QA Reader) accesses data on chips according to the most recent international standards, verifying that it has been correctly written and that it matches the printed information.

**Basic concept**

The QA 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 operator 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. Data is then read from the chip, and validated against a specific set of standards depending on the particular type of document. For instance, in case of machine readable travel documents (MRTDs), such as passports and residence permits, the document is checked using ICAO’s Doc 9303, and if applicable, the Extended Access Control specification by the BSI. In general, the rule set used to check a given document family can be tuned depending on the purpose of a particular QA Reader installation.

Once a document is processed, the operator is notified of the validation result. If the document was successfully validated, the information retrieved from the chip can be examined, as well as the detailed operation log, along with the performance indicators gathered during the check. Conversely, if the document validation fails, a succinct explanation of the failure is given to the operator, and additional information is provided on lower-level screens so that the root cause of the failure can be determined.

In terms of security, the integrity validation trust points (such as the Country Signing Certificates used during Passive Authentication, as defined in Doc 9303), as well as the credentials required to access sensitive information stored in the documents (such as the Inspection System private key, as defined in EAC) are securely stored in a tamper resistant container which is transparently accessed by the QA Reader Terminal and can be managed using the QA Reader ancillary utilities.

The QA Reader Operator interface is designed with simplicity in mind. For this reason, it is executed on a machine with a touch sensitive screen. Its main window showcases optical captures taken from the document, the cardholder portrait, and his/her fingerprints as retrieved from the document chip.
Benefit

The QA Reader can be used immediately after document personalization to ensure that the document is conformant to applicable standards. It can serve as an early-warning system to alert operators in case that something in the personalization workflow is not working as intended, thus reducing the chance of improperly personalized documents leaving the premises.

The IBM QA Reader is also useful as a diagnostics tool, for example, in case of failures due to problems with chip hardware, or incorrect/expired cryptographic material being used during the personalization process.

Key Features

- Support for contactless chips (ISO 14443).
- 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).
- Support of user roles: operator, administrator, crypto-custodian.
- Validation of the card’s Machine Readable Zone (MRZ).
- Comparison of printed card information with data stored on the chip.
- Simple user interface designed to minimize operator interaction.
- Touch sensitive screen to facilitate operator interaction and avoid peripheral clutter.
- Display of optical captures from the document taken under visible, ultraviolet, and infrared light*.
- Display of photo from chip**.
- Display of fingerprints from chip (partially obfuscated) **.
- Default high-level views of QA results.
- Detailed validation diagnostics available for root-cause validation failure analysis.
- 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.

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

*The precise amount of captures depends on the capabilities of the Document Scanner.
**Provided that the document under inspection contains this information stored using a well known standard, e.g. ICAO’s Doc 9303.