

ID Authentication in Banking Applications

Contents

- ID Authentication in Banking Applications 1
 - Current ID Verification Practices at Financial Institutions 2
 - Developments in Identification Documents 3
 - Applications of ID Card Imaging..... 4
 - Application of ID Scan/Archive and Authentication in Financial Institutions..... 4
 - Application of ID Scan/Archive and Authentication in Alternate Financial Services Channels 6
 - Future Technology Advancements – UV and Color Imaging 6
 - Exhibit A: Ohio and Georgia Drivers Licenses 7
 - About..... 8

Global financial institutions are faced with a growing need to “know” – identify and authenticate – their customers, to prevent fraud losses, the funding of terrorism, money laundering, and tax evasion. Failure to comply with proper identification of the institutions customers can result in monetary losses, fines, and bad publicity.

Current ID Verification Practices at Financial Institutions

Financial institutions typically verify ID for the following types of transactions:

1. Account Opening: The Patriot act initially required institutions to retain a copy of the ID presented during the account opening. This was subsequently reduced to requiring only the recording of key information proving that ID was verified (e.g. driver’s license number). While it may suffice to note the ID number, a simple clerical error, such as transposing numbers may invalidate the proof of the ID verification. Capturing the ID card during the account opening process confirms that the ID was verified, and opens the door for better subsequent interactions with the customer. Possibilities include:
 - a) Adding the photo ID to a bank-issued debit or credit card, without the need for photo capture equipment. Small photo IDs are used by warehouse clubs in combined member/credit card applications.
 - b) Showing the ID/photo, personal characteristics, and signature to the teller during a transaction to reduce ID fraud.
2. Routine Transactions: Machine-readable identification cards (ID cards, credit/debit/ATM cards) can be used to identify a customer. The teller application can pre-populate information about the customer to speed up the transaction, and to create a more pleasant customer experience.
3. Cash Withdrawals: ID cards are typically required for any cash withdrawal by a customer at a branch unless the withdrawal is at the customer’s home bank and the customer is personally known to the bank employee.
4. Large Transactions: Financial institutions typically require multiple pieces of ID for transactions over a certain amount threshold, including transfers and deposits. This is necessary because losses can occur with large deposits (such as cashier’s checks) where the deposit is a forgery, but only detected after the amount was withdrawn.
5. Check cashing: A recent FDIC surveyⁱ showed that 7.7% US households are unbanked, and over a quarter — 25.6 percent — of all households either don’t have a checking or savings account at all, or have a bank account but still choose to rely regularly on “alternative financial services” like payday lenders and pawn shops. Serving these customers can be profitable, especially in a tough economy, but require solutions to positively identify a person who is not a customer of the financial institution. This business is today largely handled by check cashing stores, pawn brokers, but increasingly viewed as an opportunity to bring customer into stores (such as convenience stores and gas stations) by offering check cashing services. In check cashing applications, the ID card is required for initial account registration and for subsequent check cashing transactions.

6. Government Regulations: ID verification is required for any financial transaction that may require government reporting, such as in the US cash transactions over \$10,000. In countries with foreign exchange regulations, transactions need to be reported by government ID number. Most foreign exchange windows require a valid ID.

Developments in Identification Documents

Post 9/11, it has become evident that government-issued identification (passports, national ID cards, driver's licenses) were not sufficiently protected against forgery. The 9/11 Commission recommended that the U.S. improve its system for issuing identification documents, urging the federal government to set standards for the issuance of sources of identification.

For international travel, the International Civil Aviation Organization (ICAO) issues a standard for **biometric passports**, or e-passports. E-passports include biometric information on the passport holder on a secure chip. Public key infrastructure is used to authenticate the data stored on the passport chip. The United Statesⁱⁱ and most of the EU nations have adopted e-passports for all new passports issued.

Passports are only required for international travel, and are not typically used as ID in domestic commercial transactions where state-issued **driver's licenses** are the primary identification documents.

The design of state driver's licenses has typically been insecure and very easy to forge. The easy availability of counterfeit state ID documents creates a problem with ID theft, and the enforcement of liquor sales restrictions.

In 2005, President Bush signed the Real ID—"Improved Security for Driver's License and Personal Identification Cards" Actⁱⁱⁱ. Real ID has been controversial, with several states demanding a repeal and replacement with the proposed PASS ID act. As of January 2011, Department of Homeland Security issued a waiver of the deadline, but states must be in full compliance by May 2011.

In addition to Real ID, Michigan, New York, Vermont, and Washington are issuing Enhanced Driver's Licenses (EDL)^{iv}. EDL's provide proof of identity and U.S. citizenship, are issued using a secure process, and include technology that makes travel easier. EDLs are an alternative document to comply with travel rules under the Western Hemisphere Travel Initiative (WHTI) for entering the United States from Canada, Mexico, or the Caribbean through a land or sea port, in addition to serving as the permit to drive. Michigan, New York, Vermont, and Washington issue WHTI compliant documents.

Despite the opposition to REAL ID, most states are implementing new driver's licenses and state ID cards that include enhanced security features:

- **Magnetic stripes** – magnetic stripes have been the main method for storing information on a credit/debit/ID card. They are not very secure, but are usually retained for compatibility with a large installed base of equipment.
- **2-D barcodes**. EDLs require a Machine-Readable Zone (MRZ) or barcode as backup to the RFID. Many states are adopting 2-D barcodes in basic driver's licenses. 2-D barcodes (see Exhibit A – Ohio / Georgia Driver's License) can store more data, and data can be protected with encryption or digital signatures.

- **Radio Frequency Identification (RFID) chips.** RFID is used for Enhanced Driver's Licenses and the Trusted Travelers Programs (NEXUS, SENTRI, and FAST).
- **Ultra Violet Zones.** UV zones contain invisible symbols that light up only in the presence of UV light. These are difficult for counterfeiters to copy.
- **Microprint.** Microprint on driver's licenses prevents forgery. As with bank notes, microprint can be recognized with magnifiers and high resolution imaging devices and make counterfeiting more difficult.
- **Color and positioning of holder photograph.** As with banknotes, color patterns and placement are used to determine forgeries.

Applications of ID Card Imaging

The availability of scanners and software to capture ID card magnetic stripes and images open opportunities for two levels of utilization of the ID card images:

Archival storage of ID card images provides a definite proof that ID cards were presented. As noted earlier, they can provide levels of protection against ID theft by displaying images of the ID holder. Even a simple application of recognition technologies (comparing information from the card text, magnetic stripe, and barcode) will detect many common forgeries. Storing front/rear images of ID cards provide proof that the bank employee complied with the Patriot Act, obtaining the ID of a new account holder.

Authentication takes the ID verification to the next level. Authentication solutions offer an automated approach to ID verification, alerting the user of potential risk factors, forgeries, and expired ID cards.

Advanced ID detection systems (see example: advancediddetection.com), typically include a color/high resolution scanner combined with software to authentic ID cards. ID authentication solutions

- Scan the ID in color, with high resolution
- Read barcodes and magnetic stripe data
- Verify infrared patterns
- Cross-check information in clear text, barcode and magnetic stripes
- Warn if the ID card is expired, a person is under legal age, etc.

Automated authentication systems are used, for example, in liquor stores and restaurants to avoid sales to minors. It is interesting to note that the Transportation Security Administration (TSA) has not implemented automated authentication on a wide scale. TSA has accepted bids for systems, but so far has limited ID authentication to office training and hand-held UV lights.

Application of ID Scan/Archive and Authentication in Financial Institutions

Most teller stations in financial institutions are equipped with a validation/receipt printer, a PC, monitor and keyboard. More advanced institutions deploy cash dispensers, cash recyclers, coin recyclers, and signature/PIN pads.

Check image capture has moved largely from centralized proof/reader/sorter operations to branch capture. A majority of financial institutions have implemented branch capture (est. 68% of branches) at the back counters. Back counter capture eliminates the "prime pass" but does not eliminate most of the

back-office check processing tasks. It offers few fraud prevention opportunities – by the time the item is captured the person will have left the branch.

Fewer but more technologically advanced institutions have implemented check capture at the teller. Implementations of teller capture are growing rapidly in 2010/2011 with many major regional institutions adopting teller capture.

Unfortunately, current teller scanners are not suited for ID capture, and even less for ID authentication

- First generation check scanners were oriented towards the “lowest common denominator”, 200 dpi bi-tonal images, which may be sufficient for check image exchange but not well suited for IDs.
- The installed bases of devices have a u-track design that cannot process stiff items such as IDs.

Teller scanners are designed for a five year life cycle, but with declining check volumes will last 7-10 years or longer. It is therefore essential for the industry to ensure that the next generation teller scanner is more versatile to protect the substantial investment required to implement teller capture.

The currently available free-standing solutions for ID authentication are not well-suited for branch banking, because

- ID authentication solutions are not integrated with other banking applications
- Free-standing ID authentication solutions are expensive and would consume valuable teller workspace.

It makes much more sense to use teller check scanners for ID capture. To enable future ID scan/authentication applications, a suitable teller scanner must offer

- A straight track for stiff ID cards. Since limited footprint and the need of 100-item hoppers and stackers require a u-shaped design, ID cards must be scanned using a “by-pass feeder” that enters stiff items after the bend, but before the front/rear cameras.
- A resolution of at least 300 dpi, with 256 gray level image capture.
- An integrated magnetic stripe reader.

The next generation of check scanning devices will allow institutions to capture ID images for

- Archival storage of proof that the institution validated the ID
- Automatic capture of customer information (name, address, age, sex) for new account opening or future marketing of unbanked / competitor prospects.
- Additional logon security by authenticating the teller using the teller employee ID card.
- Faster teller service by automatically opening the customer account when an ID or credit/debit card is captured –without an extra PC peripheral device. This is commonly used in teller operations in international banks.
- Recoding of ID images for display at teller workstations to prevent withdrawals with stolen ID
- A level of authentication supported by 300 dpi grey-scale images, such as decoding 2-D barcodes, and matching ID card and account data with barcodes and magnetic stripe information
- Potentially adding ID pictures to bank-issued Debit/ATM cards, a practice successfully used by warehouse clubs for combined membership/credit cards, without additional photo equipment.

Application of ID Scan/Archive and Authentication in Alternate Financial Services Channels

Alternative financial services channels provide services that are mostly targeting the unbanked/under-banked population. Alternate financial services are provided by pawn brokers, check cashing stores, pay day lenders, gas station stores, casinos, convenience stores, and even prisons. A recent Wall Street Journal article^v lamented that the 2009 Credit CARD (Card Accountability Responsibility and Disclosure) Act “pushed more Americans outside the banking system” in the name of consumer protection^{vi}.

Many alternate financial transactions are conducted on financial self-service kiosks. Kiosk integrator manufacture devices with a wide array of features: ID card readers, debit/credit card readers, check acceptors, cash dispensers and acceptors, cameras, and even money order and store value card printers.

Since these customers typically do not use a bank card as the ID or debit/credit card, the driver’s license becomes the primary identification tool. The following is an example of an application implemented at convenience stores of a gas station chain with the CTS SB50E module in a self-service kiosk:

- Customer registers by inserting the driver’s license. The ID is scanned, stored, authenticated by software, and returned to the customer.
- The customer is registered using information from the ID (clear text, magnetic stripe and barcode).
- The customer feeds in the check.
- The ID and photo/video of the customer is used for approval by a human operator at a central location. The operator accepts the check and it is endorsed, stamped and retained in the device, or rejected and returned to the customer.
- The kiosk dispenses cash, a stored value card, or a money order (minus a commission).

Financial self-service kiosks are funded by transaction fees, but are often deployed as a marketing tool to bring customers into the convenience store.

Future Technology Advancements – UV and Color Imaging

While color images are standard in most imaging applications, they have not been widely adopted in US check processing. But in international banking, the use of color imaging and UV is growing rapidly.

- Asian applications require higher-resolution color images to authenticate “chops” - seals that function as signatures.
- Central banks in India^{vii} and Latin America are establishing check standards that include UV zones to prevent fraud. The new Reserve Bank of India Check Truncation System CTS-2010^{viii} features include use of watermark and printing of bank logos that are only visible with ultra violet images.

As a result, we will see advancements in check scanner technology, including UV and color image capture for check capture and authentication. Color / UV image capture will offer the opportunity to further improve the strength of ID authentication.

Exhibit A: Ohio and Georgia Drivers Licenses



About

About CTS North America

CTS is a group of three privately-owned companies: CTS Electronics, CTS CashPro, and CTS North America. CTS Group is a technology company focused on the development, production and support of systems for electronic payments. CTS has global coverage with more than one million banking peripherals installed across five continents, a proven track record in major global financial institutions, and partnerships with the most prestigious solution providers in the industry.

CTS offers a wide range of products for banking and financial applications involving document imaging (read, scan, encode), cash handling systems, card personalization and self-service modules.

The **CTS LS150** has the smallest footprint / throughput ratio on the market today. Its fast and quiet performance, coupled with its sleek design and unique features make it the superior choice for teller, branch, and high volume remote deposit capture applications. The LS150 provides reliable check scanning needed at teller stations today, and investment protection with advanced features and speed that will be needed in the future:

- 75 or 150 DPM (upgradeable) – the fastest scanner in its class can eliminate deferred deposits
- The smallest footprint on the market - highest throughput to size ratio
- An auto retracting feeder— single handed insertion of up to 100 item batches without losing eye contact with your customer
- Very low noise emission
- A bypass feeder for image-only documents and IDs
- Magnetic Flip Open Doors — easy cleaning and maintenance
- Lower TCO with no operator replaceable parts or cleaning cards needed.

The **CTS SB50E** and the **LS400F** are modules designed for integration in a self-service kiosk. The SB50E is a robust scanner designed specifically for challenging self-service applications. The SB50E accepts ID cards, creates a high-resolution color image (300 dpi) for data extract, archive, and authentication. The same track and image camera reads (MICR) and scans checks (front/rear) and optionally applies front stamps or rear endorsements for accepted checks. The SB50E tracks is bi-dimensional – returns ID cards after scanning, returns refused checks, and stacks accepted checks in a bin inside the kiosk.

About the Author:

Urs Bockli is an international marketing practitioner, with over 30 years of experience working for multinational Fortune 500 companies in Europe and in the United States. He has held a number of sales and marketing positions including Program Marketing Manager, Director of Sales Europe/Africa, Strategic Planning, and Division Director of Marketing. Urs is also a part-time Lecturer at the University of Michigan (Dearborn) College of Business.

Urs is currently EVP and GM of CTS North America, Inc., the US subsidiary of CTS Electronics SpA. In this position, Urs is driving CTS' strategy to become the top vendor for check scanning and cash solutions in North America.

Mr. Bockli has a degree of Betriebsökonom (Corporate Economist) from the Zurich School of Advanced Economics and Business Administration, and is a Certified Computing Professional and Professional Certified Marketer.

Sources

<http://www.cis.org/realid>

http://www.dhs.gov/files/laws/gc_1172765386179.shtm

<http://advancediddetection.com/default.aspx>

<http://www.ncsl.org/default.aspx?tabid=13577>

http://www.dhs.gov/xnews/releases/pr_1223915151497.shtm

http://www.dhs.gov/files/crossingborders/gc_1161636133959.shtm

http://www.michigan.gov/sos/0,1607,7-127-1627_8669_53333-213055--,00.html

ⁱ <http://www.economicinclusion.gov/>

ⁱⁱ http://travel.state.gov/passport/passport_2498.html

ⁱⁱⁱ http://www.dhs.gov/files/laws/gc_1172765386179.shtm

^{iv} http://www.getyouhome.gov/html/lang_eng/eng_edl.html

^v Wall Street Journal, Jan.4 2011, Todd Zywicki, Dodd-Frank and the Return of the Loan Shark

^{vi} Dodd-Frank and the Return of the Loan Shark – Todd Zywicki, Jan 4, 2011

^{vii} <http://indianbanks.org/tag/reserve-bank-of-india/>

^{viii} <http://rbidocs.rbi.org.in/rdocs/content/PDFs/SCFR220210.pdf>