Digital Authentication of Documents

Essential to Combatting Global Counterfeiting

Table of Contents

Executive Summary

People and high value manufactured products move across borders very quickly in the present day. This increased freedom of movement brings with it increased opportunities for transnational criminal organizations. Among the most profitable and lowest risk criminal enterprises are the counterfeiting of manufactured products and the counterfeiting of identity documents.

Manufacturers routinely use digital authentication to protect their branded products and to reduce the risk of counterfeited component parts. The complimentary investment in digital security features adds protection to object authentication. Government security and law enforcement agencies are increasing deployment of digital authentication to reduce imposter risk to public safety, but the pace needs to accelerate in order to reduce the time cost to travelers. While many foreign governments employ digital authentication of identity documents, our own federal agencies nearly always continue to rely on the human eye.

International travel and commerce, domestic public safety, and highway safety all depend on reliable identity verification. Pilot deployments by the Transportation Security Administration (TSA) of identity document authentication via digital devices, combined with biometric comparisons, are in their early stages. If these prove cost effective and expedite traveler screening, the business case will be made for use of digital authentication enhanced by biometric identity technologies. This will demonstrate a clear value proposition in that decreasing traveler screening costs and travel delays through digital authentication will save money without compromising security. Digital authentication can also be deployed for rail travelers without slowing travel.

This paper offers support that digital authentication will more reliably and more rapidly validate today's physical driver's licenses, passports and other secure identity documents than reliance on the capabilities of human eye and touch.

DSA

DOCUMENT SECURITY ALLIANCE

The Document Security Alliance (DSA) is a not-for-profit organization focused on document security at all levels of government to enhance our nation's economic, personal, and homeland security for the 21st century. DSA's goal is to leverage our government and industry members' expertise to identify methods of improving security documents and related procedures to combat fraud, terrorism, illegal immigration, identity theft, and other criminal acts.

Introduction

When people hear the term "document examiner," many will relate it to a television story featuring detectives from the FBI or Homeland Security Investigations. "NCIS", currently one of the most popular "detective solves crime" shows, often features document examination in high tech laboratory settings in order to root out cleverly deceptive culprits.

In everyday life, unlike in "NCIS", most document examination takes place far more routinely outside of police labs. Motor vehicle agency counter clerks verify identity and residence, social services personnel examine IDs *to determine benefits eligibility, and retail clerks confirm age suitability to purchase alcohol or tobacco products. In Colorado, California, and other states where sale of marijuana is allowed and legally regulated, ID verification is required for purchase. Similarly, in Arizona and some other states, your ID is "examined" before you can purchase cold and flu medicine that contains chemicals that can be reprocessed for illegal methamphetamine production. Large pharmaceutical chains incorporate proprietary bar code markings to automatically require clerks to verify IDs prior to sale of a range of restricted products, especially the sale of alcohol and tobacco.*

The use of digital authentication of documents that hold personal identity information in preference to the human eyes of a clerk or trained document examiner is a relatively recent technology change. Wide use of computer equivalent smart phones and tablets has raised awareness that identity protection should extend to important personal documents, like driver's licenses.

The increasing sophistication of counterfeiters that specialize in identity documents, like passports and driver's licenses, combined with the convenient anonymity of internet sales, is a growing threat to public safety. The 21st century risk from violent terrorist attacks is facilitated by the ready availability of counterfeit driver's licenses. While adolescents seek fake IDs to enter age-restricted venues or buy age-restricted items, terrorist suicide bombers seek them to rent cars they will load with explosives and detonate in public areas. This terrorist methodology is demonstrated almost daily by suicide car bombings in Middle Eastern countries and Europe, killing dozens of civilians at a time.

The document security industry has responded to those 21st century challenges by creating new security features, improving on industrial methods for time tested features that already exist, and devising new technology assisted software and mechanisms to authenticate a broad range of documents.

Business and Societal Risks from Borrowed or Counterfeit Driver's Licenses and IDs

Technological advances, including new types of digital image capture, photo manipulation popularly known as "photo shopping," and increasingly sophisticated software, have changed popular culture. But these innovations also make it easier and cheaper to counterfeit valuable identity documents, currency, and product labels that convey quality and safety. Although it's not immediately obvious that currency and the labeling on common products are documents, they are in fact printed materials. To keep document integrity and protect currency and product value, governments are constantly upgrading secure document materials to stay ahead of counterfeiters.

The introduction of automated teller machines (ATMs) in the United States and Europe roughly thirty years ago was the major contributor to the sophistication of digitized security features included in currency. Since the earliest days of automated deposit of currency in vending machines and ATMs, counterfeiters have often successfully substituted counterfeits that fooled the counting capacities of the machines.

Currency continues to get the greatest focus by counterfeiters, and banks and government agencies combat them by introducing new security features that include digital refinements. Many millions of daily commercial transactions rely on ATMs and high value vending machines which incorporate sophisticated digital authentication devices that verify currency and reject counterfeit and damaged documents.

This technology is important in order to:

A. *Facilitate the positive authentication of the document and the data contained on it in real time;*

B. *Identify altered documents;*

C. *Identify fictitious and counterfeit documents;*

D. *Enter newly created valid documents into a system and exclude documents that are malformed or inaccurate;*

E. *Take incorrectly printed, damaged, or destroyed documents out of a system (example: quality control readers for chip enabled passports are employed by government agencies prior to personalization of the passports).*

Adapting Technology to Improve Identity Verification

The most common technology assisted documents routinely examined in the United States are banknotes, otherwise known as currency, followed by machine examination of transit tickets used for buses, commuter trains, and subways. Due to the high frequency and high dollar value of counterfeiting currency and transit tickets, machine readable authentication is a necessary feature to quickly address service demands of millions of daily users. Another example of routinely authenticated high value documents are lottery tickets, although only the tickets presented by apparent winners are subject to authentication. Electronic scanners, both stationary and handheld, are today universally employed to read barcodes and match to known information residing directly on manufactured objects or documents. A majority of police patrol cars and state highway troopers have portable bar code scanners combined with remote access to data bases that allow for both authentication and reference to prior traffic offenses.

The proliferation of international trade agreements combined with the availability of transactional tools via internet communications facilitates the global economy. Access to foreign sourced luxury goods has improved the quality of life for those who can afford them and has improved the profitability of those who provide such goods. It has also created a new worldwide industry of making and trafficking counterfeit branded products that is highly profitable and difficult to police.

For more than a decade, in order to protect their business brands, manufacturers and legitimate retailers have had little choice but to add sophisticated security markings onto labels and merchandise tags. Increasingly, hidden security features are placed within the products, including microchips that activate only specialized chip readers and send coded signals. These security markings and hidden chips can be authenticated by electronic devices when goods are received at warehouse or retail outlets. Very often, digital security features are chosen because they can be printed along with brand and model information that is used for inventory management so a merchandise item will only need to be scanned or "read" by a device a single time. Examples of other high value, routinely examined documents subject to counterfeiting and now potentially applicable for automated authentication include passports and state-issued driver's licenses. Other identity documents which are routinely examined by agencies assisted by digital data analysis devices include birth certificates, death certificates, military identification documents, federal government (HPS-12) IDs, concealed carry and handgun permits, company employee IDs, and, in more than 30 states at least every two years, voter IDs.

Documents printed on paper or on plastic composites are traditionally authenticated with visual examination by trained document examiners and by validating issuance details with the document providers. Valuable paper and plastic documents that prove eligibility for rights and benefits contain prominent visible security for authentication by the trained human eye. Increasingly, technology authenticatable security features and embedded chips are added to vehicle registration stickers, safety inspection stickers, medical records and hospital IDs for patients and employees, welfare and food stamp debit cards, and many other valued items. In recent years, automated authentication methods have emerged, including the pairing of lower cost, high resolution digital cameras with mathematically enhanced algorithmic software to produce digital authentication technology that rivals the highest level of human forensic examination and authentication.

DSA

It can be anticipated that future "digital" enabled tools will gradually replace traditional methods to authenticate paper and plastic documents, especially for the examination of identification cards in high security environments. A collateral validation methodology of inserting radio frequency identification (RFID) devices, like silicon chips, into documents as a security feature that can be quickly authenticated is also evolving and becoming more common.

Human document examiners also can exercise judgement when employing match comparison to referenced exemplar or other data references. Trained document examiners usually employ magnifier loupes and infrared or ultraviolet handheld light sources for close examination of security features. They are also incorporating high technology devices into their work, as described above.

Technology assisted document authentication methods in use today include:

A. *The ubiquitous bar code or machine readable zone (MRZ), which is often enhanced by encrypted security symbols to foil counterfeiters and credit card scammers. The newest bar code readers are digitally capable;*

B. *Ultraviolet (UV) or Infrared (IR) emitting or reflective light sources authenticated with UV handheld or stationary devices enabling a trained person to authenticate. The trend is toward automated small footprint workstations incorporating UV Reader or IR Sensor enabled technology;*

C. *Chemical or physical reactants which emit an observable change in color or hue when subjected to another known chemical, heat, or cold source. They are used as both a public and a forensic feature to visually authenticate paper and polymer identification cards.*

D. *Video Spectral Comparison (VSC) workstation, which is an imaging device that allows a document examiner to non-destructively analyze inks, to visualize hidden security features and to reveal alterations on a document. High technology devices used by examiners in federal law enforcement laboratories include digital Scanning Electron Microscopy (SEM), laser scanning, soft x-rays, Fourier Transform Infrared Spectroscopy (FTIR) Analysis to identify specific chemical components, and thin layer chromatography (TLC,)which is a chromatographic technique used to separate the components of a document using polarity.*

E. *RFID electronic device located on label affixed to document or embedded in ID card body.*

Secure Document Examination Is Becoming Routine

It is advisable and an increasingly common component of law enforcement training to provide explanations and document examination exposure. Some states require, and nearly all states encourage, training of retail clerks to detect counterfeit IDs and valid IDs belonging to someone else (borrowed IDs, aka "pass backs").

Today's ID counterfeiters usually have matching MRZs that will "scan" by passing through low-tech retail bar code readers. These counterfeit IDs will evade most machine device detection, whereas human eye and touch authentication by a trained document examiner can detect counterfeits missed by MRZ readers.

Recently, due to business opportunities from Department of Homeland Security requirements, several device manufacturers are offering sophisticated VSC type devices that go well beyond MRZ scanning and can detect most counterfeit IDs. These are now being deployed at high security gateways and eventually at most airports. A VSC workstation is a video spectral comparator, which uses a combination of cameras, lights, and filters controlled by software to compare the effects to known data bases of exemplars.

Increasingly, authentication of secure documents, brand labels, and especially driver's licenses includes using fixed or handheld mobile devices. Most of these new mobile authentication methods require the use of a Quick Response Code (QR Code) to allow access to encoded information on the physical or virtual document. The QR code is a digitized printed image or virtual image that has equivalency to 2D barcode standards (PDF-417). It is a standard feature which can be read by smartphone applications dynamically interacting with a secure website to undertake automated data match comparisons.

Examples of tools used to authenticate documents via fixed devices are smartphones or mobile device attachments, polarizer or magnifier. A polarizing lens can filter icons or other disturbances in laminates. A clip-on magnifier can be used to view microprint, print images, or perforations. An ultra violet (UV) or infrared light source can illuminate otherwise invisible images printed in that specific medium and/or additives incorporated within document materials or in the white areas or information blocks used as identifiers. Two of most common devices used to authenticate documents via a fixed device or mobile device such as a smart phone, or mobile device attachment, are taggant locators / identifiers and barcode scanners. The taggant identifier emits light to recognize trustmarks at specific ink / varnish locations or specific light wavelength reflections that authenticate the documents. Barcode scanners illuminate and read 2D type code for anomalies.

There are now a variety of smartphone applications that utilize the onboard high resolution cameras and internet connectivity to authenticate documents, especially identity documents. This has actually led to a new "verb" in the interactive technology industry: "onboarding," which conveys self-enrollment via a smart phone in a system for applications or services. Onboarding may also include digital authentication of a driver's license or passport for enrollment identity confirmation.

Business Case Applications of Smartphone Enabled Document Data Capture and Authentication

Capture and validate:
***A**. barcodes by matching to known data in the phone itself or via internet connection to a validation or archival data base;*
***B**. pixel manipulated artwork and relay via internet for established data for display or link to website;*
***C**. high density 2D code type data image resident on document to match/verify photo or other data visually present;*
***D**. specific image, decode on the device itself, or send data for verification, either by match or real time algorithm;*
***E**. a variable laser engraved image for further decoding, either locally on the device or through match code via connection;*

Simultaneously capture decodable image and adjacent barcode to facilitate serialization match of corresponding validated image;

i. *primary decodable image and secondary decodable image incorporated in barcode element area;*

ii. primary decodable image, barcode image, and secondary decodable image incorporated in barcode element area;

Dual authentication of two documents can be enabled by either validating images placed side by side or one after another (software determines sequence order and timing of capture reads);

Smartphone or mobile device application can locate two or more images in specific locations to determine artwork validation before directing users' devices to pre-loaded data/content or to pre-determined web portal or site;

Smartphones applications can validate "contact" authentication of printed documents using coordinates derived from multiple chemical based images. The printed image utilizes image locations in areas of document to facilitate electrical connections that onboard software detects and compares to current valid matches.

Mobile Driver's Licenses Will Be Digital (Virtual) Secure Documents

Mobile Driver's Licenses (mDL) may or may not be the wave of the future, but in a few states work is underway to determine their near term viability. The mDL can only be validated by digital authentication. A few states are experimenting with the mDL option as a means to quickly convey data on the card based credential. *However, just as the chip incorporated in today's passports is rarely confirmed for lack of chip readers, mDL deployment is years away. It will take time to perfect the data exchange and to convince the public that an mDL is a viable ID.*

State governments, including Virginia, New Jersey, Iowa, North Carolina, and Delaware, are examining the potential for mDL and other electronic verification applications to include insurance. Iowa is currently conducting a proof of concept mDL pilot enlisting state employees to test the reliability and suitability of mobile phone confirmation of driver's licenses.

The risk confronted by states considering offering an mDL as an adjunct to a traditional driver's licenses are the lack of a proven means to prevent counterfeiting, including phone hacking.

DSA

Business Case Prevention of Hacking or Message Interception

For decades there have been reassurances by the industry and the federal government that cell phones and secure data records are safe from hacking. These reassurances have been proven wrong by the highest level of system hacking yet experienced over the past four years, and encryption has become the norm to prevent it. The encryption of cell phone data will be essential for mDL adoption, and so will digital authentication to prevent electronic deception and digital counterfeits. Criminals, transnational terrorist groups and those engaged in espionage will predictably attempt to circumvent mDL security mechanisms.

State agencies studying mDL options recognize that digital authentication measures are required before deployment. The requisite ones necessary are still under study. For example, (1) knowing in real-time that the mDL is connected to the holder; (2) confirming that the information was in fact created by the issuing authority and is unchanged; and (3) omitting from view personal identity information (Pii) not necessary for the authentication purpose.

Different authorities might provide for a law enforcement officer engaged in a traffic stop to see all data on a presented mDL, while a bartender would be only able to confirm name and age. Additional details on what the mDL functional requirements are can be obtained from the American Association of Motor Vehicle Administrators (AAMVA).

Business Case Examples of Internet Connected Devices for Authentication of Digital (Virtual) Documents:

These applications typically rely on a QR symbol or secure digitized image to begin an automatic route from the authentication device to a secure website where automated interactive authentication occurs.

***A**. Smartphone, fixed or mobile device camera can be utilized to perform authentication of a digital virtual image, such as a driver's license or military identification, by sampling image(s) resident on presented device and comparing to known image data;*

***B**. Smartphone, fixed, or mobile device camera can be used to verify web pages directly on monitor to establish identity of internet derived/captured document for on-screen viewing or output printing;*

***C**. Smartphone device can simultaneously capture users' facial or other biometric attributes as dual authentication while capturing data from presented document;*

***D**. A fixed mobile device can validate virtually captured identification documents by on-device decoding of barcode and barcode elements incorporated with covert decodable identifiers.*

Digital authentication is intrinsic to the potential use of virtual identity credentials and there are new industrial product authentication uses with great potential, most of which involve inventory tags that can be inexpensively deployed and authenticated.

Conclusion

Digital authentication is helping traditional issuers of credentials add security features that are outside the range of the spectrum visible to humans or smaller than the unaided eye can recognize.

With over two billion plastic identity cards issued worldwide, secure documents will remain important to us for a long time to come. Further, there is general acceptance by people of most nations of the durability of secure plastic polymer identity cards that are impervious to interruptions of electrical power or telecommunications bandwidth.

For business and personal uses, authentication will be an essential part of acceptance of the documents, whether for product labels, currency, or identity credentials. Digital authentication can speed the process along and add reliability of great value to human enterprise.

DSA
DOCUMENT SECURITY ALLIANCE

204 E Street, NE
Washington, DC 20002
Phone: 202/543-5552
Fax: 202/547-6348
www.documentsecurityalliance.org
info@documentsecurityalliance.org

In appreciation to DSA members Brian Zimmer and David Wicker for their leadership in developing this white paper