CRAWFORD
TECHNOLOGIES

WHITE PAPER

Document Security in the Digital World

Introduction

Documents are integral to business. They contain vital information and serve a wide range of functions, both within an enterprise and as the most common and effective vehicle of communication with the outside world. In fact, one of the underlying assumptions of effective document creation and delivery is that documents must travel outside their point of origin, often multiple times.

The purpose and function of a document is virtually limitless. It can record transactions, convey confidential and proprietary information, provide timely messages, and more. But whatever the specific application, documents have always been, and continue to be, the most widely accepted “go-to” tool for conveying vital information.

Document Integrity

Ensuring that a communication is accurate, that it in fact comes from whoever is sending it, and that it has not been modified in its journey has been a key component of document delivery throughout recorded history. Some of the earliest “technology”, such as invisible inks, can be traced back to Greek and Roman times. Egyptian clay tables dating back 3500 years have been found containing encrypted information. Since the invention of paper, signatures and wax seals have been used to establish the validity of a document. Put simply, documents are the source of the indisputable truth.

However, 21st century technology has introduced a new set of risks. Virtually all communications today start and end their life as electronic documents. We take for granted that information we need can be delivered and consumed in various forms – print, fax, email, email, webpage, or any combination of these.

The PDF format has rightfully become the industry standard format for electronic documents. Rules set and maintained by an international standards board defines how content is encoded in a PDF, ensuring that the document will be rendered in a way that is consistent with the original composition, independently of the device or devices used for printing or viewing.

But PDFs in and of themselves are not secure and fraud resistant. Just like the paper documents before them, PDF based electronic documents need to be protected as they are transmitted, ensuring that the information in them is not viewed or manipulated by unauthorized recipients. With the numerous well-publicized data breaches, spoofing and phishing scams in the last few years, we are all aware of the risks that accompany the conveniences of our digital world.

The reality is that until recently digital documents have been more vulnerable than paper. The information they carry can be modified relatively easily, with no obvious change to the document’s appearance or to the presumed sender’s identity. And the consequences can be serious for consumers and businesses.

Risk Profiles for the Enterprise

Financial documents such as transactional statements contain content that automatically, and unavoidably, attracts the attention of hackers, phishers, and other “bad guys”. Although we are all aware of the value of personal information, and the importance of protecting that information, consumer protection laws have increasingly placed the responsibility of safeguarding documents containing personal and confidential information on businesses. There is direct and tangible damage if a business is not in compliance, with often hefty fines and penalties. There are the costs of programs, such as providing no-charge credit repair services to consumers who have been harmed by fraudulent documents. And then there are the indirect and less tangible costs, which can be even more insidious and long-lasting, such as damaged reputation and loss of future revenue due to reduced customer confidence.

Businesses have a fiduciary, legal and even an ethical responsibility to protect the information they possess, particularly when it is transmitted to and accessed by other people, such as their customers. Most security schemes operate at a functional level, with defined security policies, firewalls and other tools and procedures for implementation. But what is required is a strategy and solution that can operate at the practical document level, protecting each and every document wherever its life cycle takes it, inside and outside the physical and electronic walls of the enterprise.

Authentication Made Secure

With Signed PDF, Crawford Technologies provides a solution that functions at the individual document level to verify and protect the content of the document. When a PDF is created or converted from another format, the contents of the document are read and used to automatically calculate a hash, employing the most commonly used cryptographic hash algorithms.

The hash is stored, along with the customer’s public key, within the PDF as the signature. When the recipient opens the PDF, the contents of the PDF are validated by comparing the document’s hash, using the embedded public key, to the hash within the digital signature. The PDF will look like a standard PDF, but if it’s been tampered with, the digital signature will be invalidated, and the customer will receive an alert.

Alternative Solutions

There are alternative solutions which offer more limited protection, and that can be used in conjunction with Signed PDF. For example, PDFs can be protected from inadvertent access by simply specifying a password when they are created. The password protected document is relatively secure while it is in transit but is still subject to tampering by the recipient or an insider with knowledge of the password.

Documents can be digitally signed in a way that indicates who signed the document, but this is not the same as Signed PDF. This type of digital signature identifies who has created or approved a document, and can take one of multiple forms. One is a digital certificate, an identifying element validated by a third party. The level of trust in the third party (and the validation process) allows the recipient of a document with this form of digital signature to have assurance that the document comes from the source it purports to be from. This can eliminate spoofing and some other forms of fraud but the process isn't designed to secure the contents of the document – it merely identifies who sent it.

Another form of digital signature is signature capture, which uses an electronic facsimile attached to a document in place of a pen and ink signature to establish that the signer is legally signing the document. Technologies and the laws governing them vary, but the generally accepted practice is that the electronic facsimile can be used in place of a pen and ink signature. Again, the contents are not protected. In fact, there is a more significant element of trust involved as there is no third party validating the identity of the person affixing the facsimile to the document.

Summary

As a comprehensive authentication solution, Signed PDF is the most reliable format for encoding documents. It provides protection against virtually all threats, including fraud, which most other protection schemes don't address. It safeguards the documents at any point during the communication process, and most important, across all of the channels we use today.

Signed PDF applies protection at the outset of the electronic lifecycle, which then persists across each of the distribution channels, including when the document is accessed and controlled by parties outside the enterprise. From a recipient's point of view it's simple. They will receive an alert if the PDF they receive has been altered, and will know that the document may not be legitimate.

For the document provider, implementation of the powerful capabilities of Signed PDF is straightforward and flexible, with a selection of options for integration and processing. PDFs can be digitally signed in production batch mode, or on demand upon retrieval, giving the provider unparalleled automation and throughput.

Signed PDF represents a unique new total solution to document protection.

CrawfordTech Solutions

Crawford Technologies develops software and solutions to help enterprises optimize and improve the secure and accessible delivery, storage and presentment of their customer communications.

With over 1,800 customers on six continents, CrawfordTech solutions and know-how enable the largest banks, insurers, healthcare providers, utilities and print services companies to use their existing technologies, documents and data in new ways. We help them navigate the challenges in leveraging legacy applications in the platforms and applications of the future.

CrawfordTech's products, services and domain expertise reside at the nexus of content, data, and output management and are essential components of our customers' digital transformation, output management and document accessibility strategies.