NEED A MASTER PLAN?

# WHITEPAPER ON DOCUMENT SECURITY [2023]

**This approach is relevant across industries and and across all types of organizations - large enterprises, governments, small and medium enterprises, health care and educational institutions.**

Qryptal

# Whitepaper on Document Security

**Reimagining  Document Security**

## Introduction

The secure documentation industry is evolving rapidly as the world shifts towards a digital-first approach, and new technologies are embraced across various sectors. This is particularly evident in healthcare, personal identification, banking, invoicing, and trade finance[1]. However, these changes extend to other areas, including brand authentication, corporate documentation, ticketing, and laboratory certification. As digital documents become more widely accepted and used in the coming years, they will continue to drive innovation and transformation in the industry.

## Reimagining Document Security

Document security is safeguarding the integrity of a document's information to ensure trust, integrity, and authenticity. It aims to prevent the loss of information through data tampering and to establish confidence that the document is from the originating organization and has not been altered or modified unauthorizedly. Additionally, document security helps to facilitate compliance with legal requirements and smoothens economic transactions by enabling trust and integrity of the data contained in the document. Whether in physical or digital form, implementing appropriate security measures during document generation helps to preserve the integrity of the information and make it tamper-proof for the verifier while also providing an easy and efficient way to verify the authenticity and integrity of the document. This ultimately leads to greater trust and confidence in the document and its information and facilitates more efficient processing.

## Why is Document Security Important?

Document security is crucial for protecting sensitive data and maintaining trust between an organization, its partners, and its customers.

Here are 5 Reasons:

1. Data Protection
2. Trust - Building and Maintenance of Trust
3. Customer Confidence
4. Reputation
5. Risk Reduction

When handling or sharing documents in either digital or physical format, it is essential to ensure that it remains tamper-proof and secure across all communication channels and parties, including third parties. More so if it is part of an economic transaction. By implementing effective document security measures, organizations can build trust with their customers and third parties,

---

[1] https://www.zdnet. com/article/digital-transformation-in-2022-and-beyond-these-are-the-key-trends/

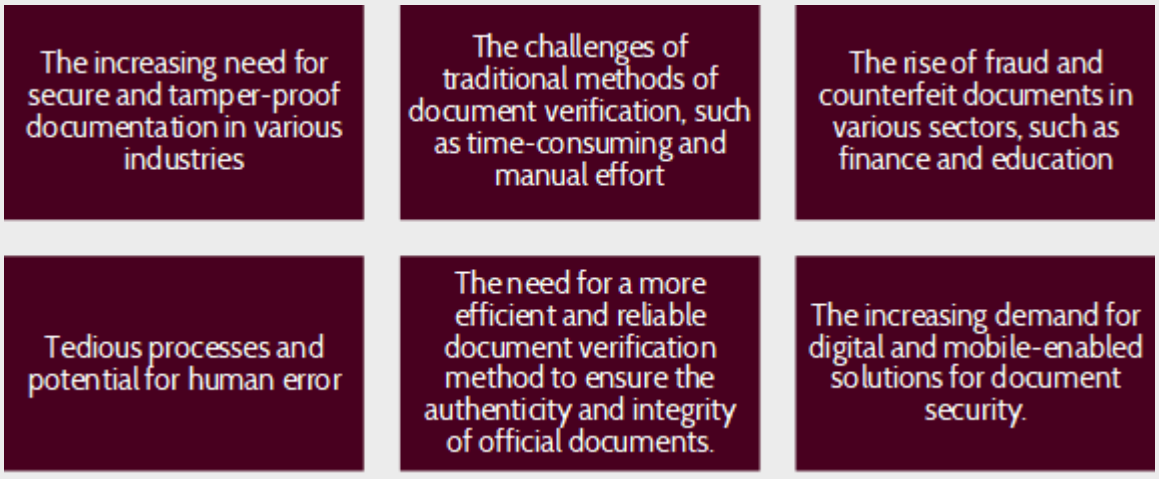
who can then have confidence in their products/services and perform subsequent transactions based on the integrity of the information. In addition, comprehensive document security measures reduce the risk of fraud, including cybercrime, as users can verify the documents' authenticity, enhancing the organization's reputation.

## Problem Statement

With the increasing reliance on digital documents and the growing need for secure communication, it is crucial to ensure that these documents' authenticity, integrity, and confidentiality are always protected.

Traditional methods of document security, such as watermarks, embossing, manual signatures, physical seals, etc., are often prone to forgery due to technological advances. Overall they have become less effective, if not obsolete, in protecting against document forgery. Moreover, with most transactions happening digitally, some methods which work well in the case of physical documents are found wanting in the digital versions and vice versa. e.g., Sometimes the physical security features are not easily verifiable in the digital versions, and sometimes it's the other way around (e.g., in the case of digitally signed PDFs, the physical printouts lose the digital signatures).

Additionally, as digital documents become pervasive, they further complicate document security, as it has become easier to duplicate and tamper with digital documents. As a result, there is a need for a more secure, efficient, and cost-effective document security method that can be easily integrated into existing systems and processes. This white paper aims to explore the various challenges and opportunities in document security and to provide a comprehensive overview of the latest technologies and best practices for securing digital documents.



## Solution for Securing Documents

The answer to the problem of document security lies in implementing various methods that can be used to secure and verify the authenticity of a document. These methods include digital signatures, secure QR codes, and blockchain technology.

Historically, document security relied on physical solutions such as holograms, stamps, seals, and embossing. These measures were effective in the past when documents were primarily physical, and the availability of such security features was limited, making it difficult to duplicate and forge such documents. However, with technological advancements and the widespread availability of these traditional security measures, they have become less effective in protecting against document forgery.

The shift towards digital documents has further complicated document security, as it has become easier to duplicate and tamper with digital documents. Digitally signed PDFs are one solution that addresses this. However, users can verify only if they have the right software on the right platforms. For example, verifying these digitally signed documents on mobile phones is difficult. Moreover, this method does not work once it is printed out and presented physically (See https://www.qryptal. com/blog/pdf_stamping/)

1. **Digital signatures** are a method of verifying the authenticity and integrity of digital PDF documents. They use cryptography to create a unique signature tied to the document and the signer. A third party can verify this signature to confirm that the document has not been tampered with and that the signer created it. However, verifying such digitally signed PDFs is a cumbersome process as users can verify them only if they have the right software on the right platforms and with some technical know-how to verify. The average person will likely not know the requisite steps to verify these digital signatures. On mobile phones, the commonly used default PDFs viewers cannot verify these digitally signed documents. Hence verification of these documents is not mobile-friendly and is designed more for desktops. Moreover, as mentioned earlier, these digital signatures can no longer be verified once the document is printed and presented physically. These solutions do not effectively bridge the gap between physical and digital documents. /
2. **Blockchain** is a distributed ledger technology that uses cryptography to secure transactions and data. It is often used to create tamper-proof records of transactions and other data, such as digital assets. Unlike digital signatures, blockchain does not directly verify the authenticity and integrity of a document. Instead, it creates a record of the document and its associated transactions on a tamper-proof ledger. While blockchain has been proposed as a means to secure documents, the resources needed, both in energy and monetary, added to the complexity of its implementation. Hence it is not a popular choice for businesses to implement.
3. **Secure QR codes** are a method of verifying the authenticity and integrity of physical documents. They use cryptography to create a unique digitally signed QR code tied to the document and the issuer. This code can be scanned by a third party to confirm that the document is valid and has not been tampered with. Unlike simple digital signatures,

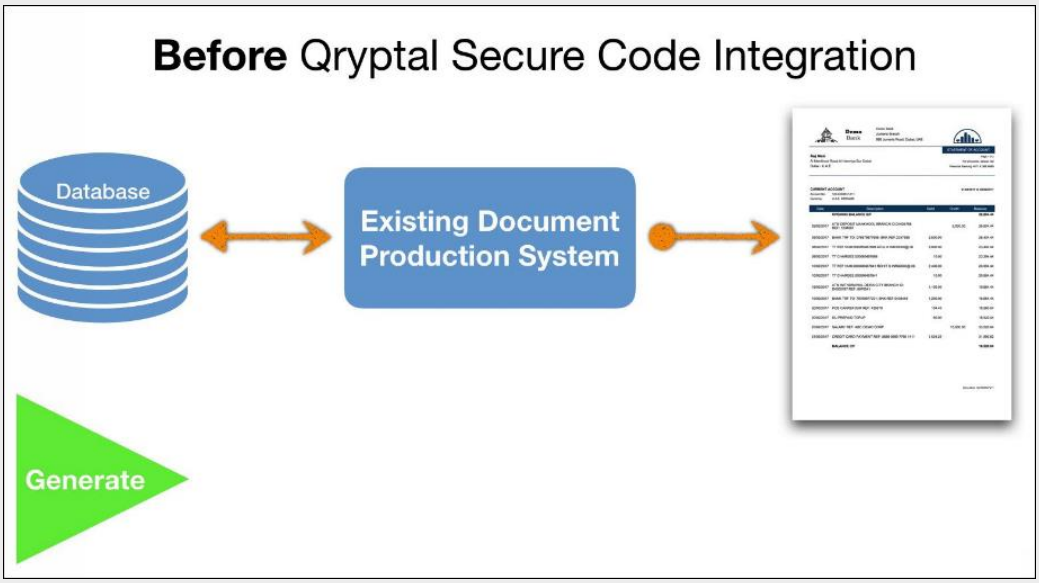
secure QR codes can be used to verify physical and electronic documents, including copies of the documents. Therefore, a digitally signed secure QR code, such as the one that Qryptal offers, offers a simple and effective solution that can be easily integrated into existing document generation workflows to secure documents.

One such cost-effective approach is PDF Stamping which Qryptal currently offers. The essential advantage is that these can be easily generated, and verification is easy on mobile devices using a mobile browser or via an app. Automated validation is also available for high-volume validations via an API. Link - PDF Stamping using Secure QR Code technology to prevent document forgery.

In summary, digital signatures, blockchain, and secure QR codes are all methods of securing documents, but each has unique advantages and disadvantages. Digital signatures help verify the authenticity and integrity of digital documents, but they cannot be used to verify physical documents. Blockchain creates tamper-proof records of transactions and other data. It's cost and complexity of implementation are prohibitive and more, so verification of the document requires the user to be online at all times. Secure QR codes help verify the authenticity and integrity of both physical and digital documents. They provide the best features of all other options and more in an easy-to-implement, use, and cost-effective package and suitable for a wide range of use cases and industries.

## Choosing a QR System That Works

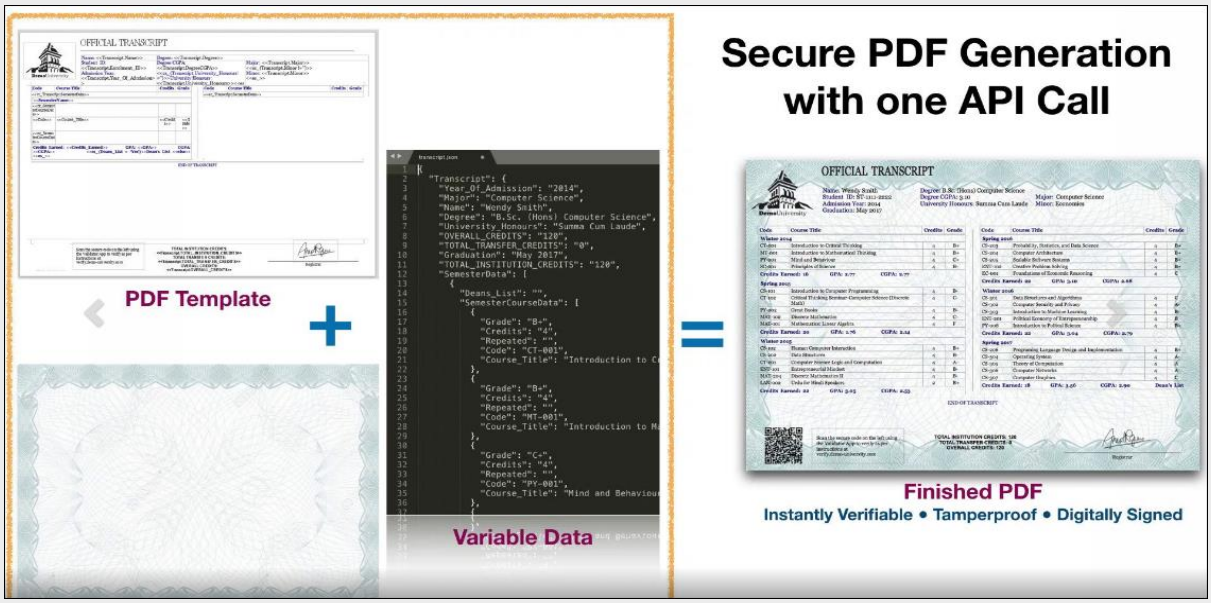
When choosing a QR system for document security, it is vital to consider the verification process's ease of use, cost-effectiveness, and universality. The system should be simple to use, allowing for the creation of secure documents in electronic and physical formats and providing an easy and universally understood verification process.




A secure QR code generator offers a cost-effective solution for quickly and easily creating many tamper-proof documents. Additionally, the validation process for these documents has been made simple and can be done across both electronic and physical formats. With the secure QR code solution, organizations can ensure the security and integrity of their documents while providing a simple and efficient way for third parties to verify the authenticity of the information.

## Implementation of Secure Digitally Signed - QR Code

Creating a secure QR code for document security is simple and efficient. Organizations can quickly implement an end-to-end solution for creating and verifying tamper-proof documents by partnering with a secure QR code service provider.




Creating a secure, digitally signed QR code can be broken down into five steps:

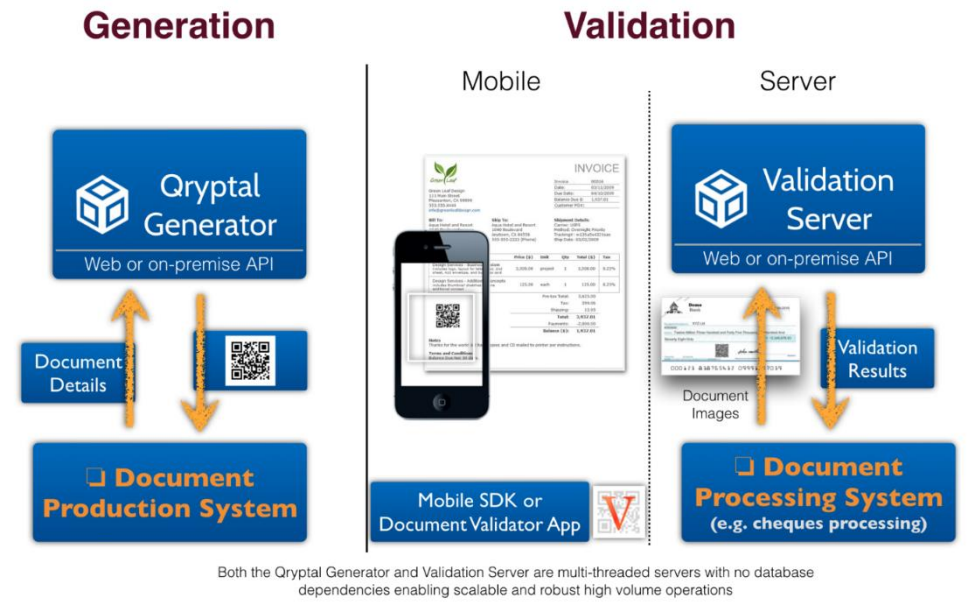
1. Contact a secure QR code service provider for an end-to-end solution.
2. Generate and Embed the generated secure QR code into your documents. Generation is available both as a manual or automated generation process via an API and fits into existing workflows. The digitally signed QR code can only be generated by authorized with the organization's private key, ensuring the code's tamper-proof nature.
3. Issue the document with a secure QR code in either electronic or physical format.
4. The secure QR code on the document can be scanned by an approved validator app or web validation mechanism, which uses the corresponding public key to validate the information and present it to the verifier.
5. The QR code can be easily verified at any time on a verification website configured for each issuer (e. g., verify.xyz.com). The secure QR code service provider will create, host, and configure this website as part of their service.

By following these steps, organizations can ensure the security and integrity of their documents while providing a simple and efficient way for third parties to verify the authenticity of the information.

## Elements of a Secure QR System

is a comprehensive solution for document security that includes several key elements. At the time of document generation, a secure QR code is added with the necessary details to verify. This information is signed by the issuer's private key, ensuring that an authorized entity generates the document. Subsequently, the document verification, which a third party may need, is done with the corresponding public key. This public key decrypts the critical information and displays authenticated content to the verifier.

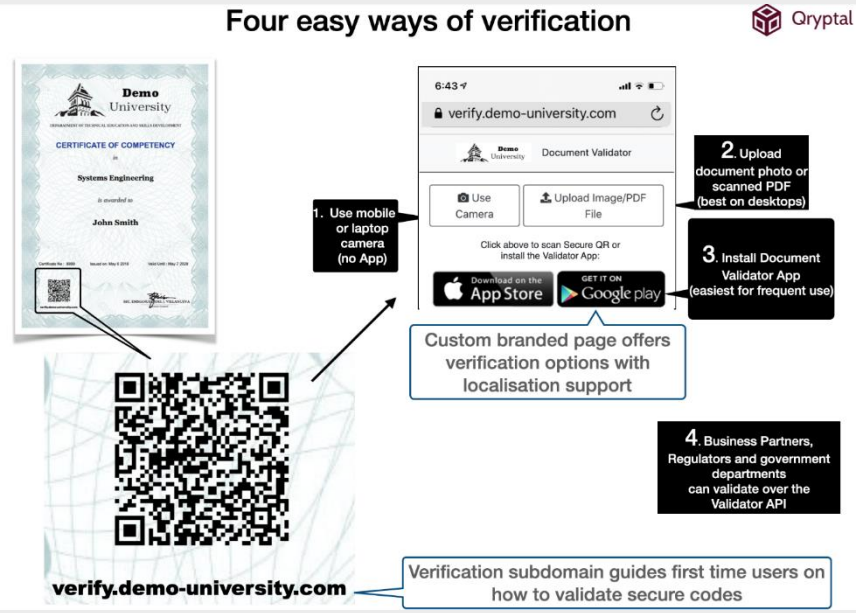
## Secure QR Code generation and validation architecture




The document production system makes an API call to the Qryptal generator with the details that need to be secured to generate the QR code. Qryptal also provides a web interface for QR code generation where the details can be input manually in case API integration is not possible or desirable. .

## Seamless Verification Experience

The verification website will offer multiple options for verification, including scanning the code with a device camera, uploading a PDF or image of the document, or installing a document validator app for iOS or Android. Automated or bulk verification methods are also available using API calls to a validation server for cases requiring bulk information processing. All the mechanisms (web validation, mobile app, validation server) have a public key that can verify the information embedded in the secure QR code, which is digitally signed by the issuer's private key. This works for both physical and electronic documents carrying the code.



## Blockchain vs. Secure QR Code


At Qryptal, we have often been asked about the use of blockchain versus Secure QR codes for secure document transfers. In reality, it need not be an either-or discussion.

Over the last decade, QR codes have grown in popularity across many applications, thanks to the widespread ownership of camera smartphones with apps that can read QR codes. This has led to an explosion in its usefulness in marketing, secure documents, and, more recently, in contract tracing for COVID-19.

However, the standard QR code faces a few challenges when security and secure document transfers are involved. Even today, QR Codes are commonly used for URL redirection to a web page or resource. However, this can lead to QR phishing and is unsuitable in case of security and making the information tamper-proof. At Qryptal, we designed our Secure QR code solution to have the information secured by digitally signing it with a private key of sufficient strength so it cannot be tampered with. The EU also used this approach to digital signing in the COVID vaccination certificate. To learn more about Qryptal's involvement in that project, download the whitepaper here: https://www.qryptal.com/whitepaper/eudcc/

Similarly, blockchain technology has risen in popularity recently for its potential uses beyond its original application in cryptocurrency, such as smart contracts and trade finance.

Secure Digitally Signed QR codes, such as those provided by Qryptal, are tamper-proof and can be considered lust like the immutable ledger in a blockchain. However, an added benefit is that the validator-user can still validate the information without being part of a blockchain network, as the verification is decentralized. -

In summary, Secure QR codes combine the best of both worlds - the high density of information per unit area of QR codes and the tamper-proof and decentralized validation of blockchain technology - at a fraction of the cost and energy usage. They can be used in various applications such as cheques, ID cards, invoices, passports, school certificates, trade finance documents, vaccination certificates, Covid test reports, etc. Additionally, enterprises can benefit from integrating their ERP systems with the Secure QR code solution through APIs. The secure QR code generation system can be deployed on-premises or in a cloud environment.

In conclusion, the increasing need for secure and tamper-proof documents in today's digital world has highlighted the importance of effective document security solutions. - Methods such as digital signatures, blockchain, and Secure Digitally Signed QR codes have been proposed as solutions, but each has its uses and limitations. Secure QR codes, in particular, capture the best of the other options and, in addition, are the most efficient and cost-effective solution for document security. With its ability to provide secure and tamper-proof documents in electronic and physical formats, and its ease of verification and validation, secure QR codes are the preferred solution for organizations and individuals looking to secure their documents. The arguments presented in this whitepaper demonstrate that secure QR codes are a reliable and practical solution for document security. As the use of digital documents continues to grow, it is essential to adopt practical solutions such as secure QR codes to ensure the integrity and security of these documents.

## About Qryptal

Qryptal is a leading provider of secure QR codes for document security, with a proven track record of success in over 30 countries. Our secure QR code solutions are used by large enterprises, SMEs, and governments to secure a wide range of documents, including invoices, purchase orders, bank statements, industrial test certificates, Covid-19 test reports, university degrees, and transcripts.

Our secure QR code solution utilizes PKI-based security equivalent to 3072-bit RSA, along with multi-stage pipeline compression to generate a small QR code footprint, making decentralized validation using just the public key possible. This technology uses standard cryptography and enables quick, efficient, and effective verification, making it a compelling solution for making documents tamper-proof and easily verifiable.

At Qryptal, we are dedicated to providing innovative and effective mobile-enabled products and solutions to businesses of all sizes. Our solutions are designed to meet the needs of today's digital world, and we are committed to helping our customers to secure and protect their critical data and documents.

## About the Authors,

Vinod Vasnani is the Co-Founder and COO of Qryptal. He has extensive experience in R&D for large and small organizations and believes in listening to customers to meet their needs. Before Qryptal, he was VP of Engineering at Accellion and held various positions at Emerson Process Management. He holds a BEng and Ph. D. from the National University of Singapore. https://www.linkedin.com/in/vinodvasnani/

Rahul Sinha is Head of Business Development at Qryptal, where he's focused on finding applications and use cases for the company's technology in different sectors. He has experience in the financial services and global markets and has worked at ICICI Securities, J. P. Morgan, and Mackenzie Investments. He holds degrees in Mechanical Engineering and Business Administration. https://www.linkedin.com/in/rahulsinha30/

Rajesh Soundararajan is CMO at Qryptal, helping customers make informed decisions on document security through digital communication channels. He has 27 years of experience in product, incubation, sales, and business. He has held leadership positions at IBM, Microsoft, and NComputing and founded Futureshift Consulting in Singapore. He has an Engineering degree, MBA, and experience in product strategy, partnerships, business development, and sales across geographies. https://www.linkedin.com/in/rajeshsound/

# CHARTING THE FUTURE FOR GLOBAL DOCUMENT SECURITY.

Qryptal provides cutting-edge document security, solutions delivering high value for our clients. Our architects have decades of experience in document security - online and offline. Our speed, efficiency, and eye for functionality make us the undisputed number one.

Learn more at -
www.qryptal.com

info@qryptal.com

+65 9298 8759
105, Cecil Street, #15-02
The Octagon, Singapore
069534.

Qryptal