WHITEPAPER

Securing Documents through PKI & QR Codes

Prevent forgery of cheques & other documents using Digital Signatures embedded in QR Codes

Forgery of documents has been a big worry for many government departments, corporates and private entities. With the technological advancements, it has become much easier for the fraudsters to mimic original documents and the tools used to detect the flaw have become obsolete. Due to sophistication in forgery techniques, it has become very difficult for the Governments to bring the culprit to the justice and also because of these corporate houses are losing revenue and more importantly having a negative impact on the brand value. In order to prevent forgery of documents, a method is proposed that can mitigate the risk of forgery and gives confidence to the individual/entity honouring the documents. The method involves secure QR Codes that contain digital signature data signed using entity/Individual's private key.

CHALLENGE

The cases of fraud & forgery of documents has increased many folds with the advance technologies that are available at cheaper costs such as printers, scanners, editing tools etc. Due to this, it has become very difficult to as certain integrity of the document.

The documents that fall prey to forgery includes (not limited to):

- Appointment letters, Experience letters, Relieving letters, Offer letters etc.
- Certificates like Graduation Certificate, Mark List etc. issued by Universities
- Invoices
- Negotiable Instruments like Cheques
- Stamp Papers
- Policy Documents
- Purchase Orders

The manual verification of these documents is a tedious & time consuming task as it involves multiple people & organizations to be contacted. Hence it is necessary for individuals/entities to adopt a technology that can ensure security & integrity of information & also provide authenticity to the documents issued. The technology also should make it easier for the entity/individual to verify the integrity of the document real time. In this ecosystem, there are three main entities or individuals involved.

They are:

- Document issuing authority. This can be an Individual, an Entity or a Government Department.
- Document holder. Document to whom it is issued.
- Document Verification carried out by an Individual, an Entity or a Government Department.

The technology that needs to be adopted should support environments like physical paper as well as electronic. The proposed product enables to combat this menace by embedding secure QR codes containing digital signature of the individual/entity issuing the document and it enables verification of the document without depending on the document issuing authority just by scanning the QR code using QR code reader apps available in various app stores.

Digital signatures are widely used at all levels like network level, database level, application level as well as for user authentication to key sensitive applications.

FACT

“It is estimated that the likely annual cost to the global economy from cybercrime is more than $400 billion"

- Mcafee Report 2014

Digital signatures are globally accepted and are purely based on publicly available standards and algorithms. These signatures link the data to the identity of the signatory, ensuring that manipulations would be detected and forgery is prevented while providing authenticity and integrity of the information it also provide non-repudiation.

In order to print digital signature on paper documents, the documents need to be machine readable to start for which QR Code is used. The data and digital signature can be encoded in a QR Code and the same can be embedded on the document and any person who wants to verify authenticity of the document can scan the QR Code by using QR Code reader app installed on the smart phone. The advantage of this proposed product is that the documents will not rely on the manual verification which is a tedious and cumbersome task. This product is so effective that the document whether it is in paper form or digital form both can be verified real time using a normal QR code reader application.

SOLUTION

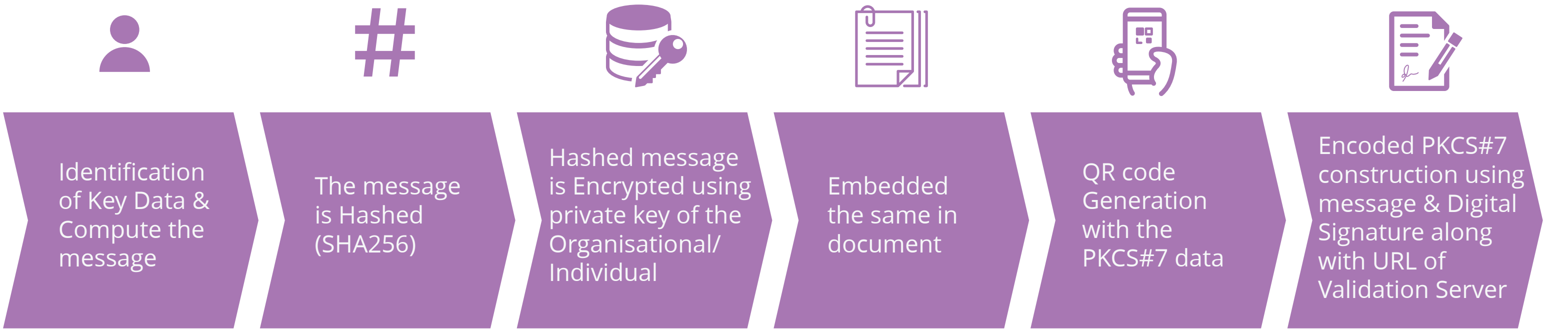
Following steps followed for preparation of document with Secure QR Code with digital signature.

- Dynamic or key information from the data on the document is converted to a message.
- The message is then hashed using SHA256 hashing algorithm
- The hashed message is then signed using the individual/organization level digital signature certificate available on the server in secured form like on HSM i.e. FIPS 140-2- level 3/4. The private key of the individual/organization available on the HSM is used to encrypt the HSM thus computed and the output of the process would be a digital signature.
- The message along with digital signature is constructed in PKCS#7 format along with URL of data validation server hosted and the same is fed to QR Code generator. The system also makes an entry of message and digital signature in the database of the entity/organization.
- The QR Code generator produces a QR Code which stores the message and the digital signature in the form of PKCS#7
- The QR Code is then embedded on the document either at the bottom of the document or at the top of the document.

FACT

“Paper checks are the most targeted payment method in the Banking Industry. It accounts for 77% payments fraud surpassing wires and credit/ debit cards which account for 27% & 34% respectively.”

- 2015 AFP Payments Fraud & Control Survey


Identification of Key Data & Compute the message
The message is Hashed (SHA256)
Hashed message is Encrypted using private key of the Organisational/ Individual
Embedded the same in document
QR code Generation with the PKCS#7 data
Encoded PKCS#7 construction using message & Digital Signature along with URL of Validation Server

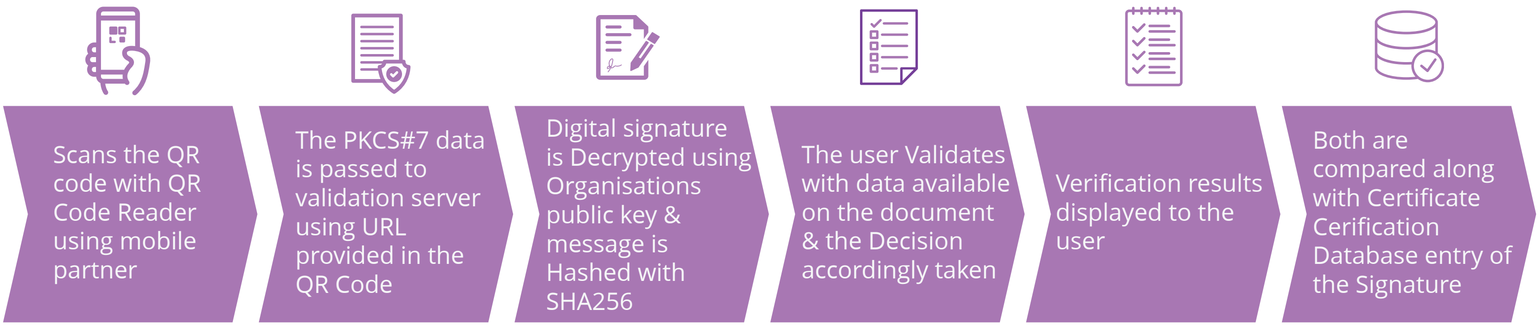
Following steps followed for authentication of document:

- The individual/organization user who wants to validate the authenticity of the document needs to open QR Code reader app available on the mobile. Many freely downloadable QR code readers are available app stores of various mobile operating systems like Android, IOS, Windows etc.
- Once the user scans the QR Code using the QR Code reader then the user is redirected to the URL mentioned in the QR Code along with the encoded PKCS#7 data.
- The server takes the data and uses public key of the organization to decrypt the digital signature and derive hash of the message and in parallel the message is taken from the data passed and is hashed with SHA256 algorithm.
- The new hash value generated using the message & decrypted signature's hashes are compared.
- If both the values are identical then it assures the integrity of the message & it also confirms that the document was generated by the said individual/authority only.
- The organization certificate is also validated for its expiry, issuer and CRL/OCSP.
- Apart from the above verification, the server also checks whether there is an entry in the database for the given digital signature.
- Once the digital signature is successfully verified the original details based on which the signature was created is displayed to the user to verify the same with details provided on the document.
- If both the details are matching then it's a valid document otherwise it can be concluded that the printed document has been modified.

FACT

"BFSI sector is the top target for cybercrime, accounting to 74% of overall cybercrime in India. And about 63% amounted to financial loss."

- Cybercrime survey report 2015 - KPMG



Scans the QR code with QR Code Reader using mobile partner

The PKCS#7 data is passed to validation server using URL provided in the QR Code

Digital signature is Decrypted using Organisations public key & message is Hashed with SHA256

The user Validates with data available on the document & the Decision accordingly taken

Verification results displayed to the user

Both are compared along with Certificate Cerification Database entry of the Signature

The solution therefore provides for:

- 100% elimination of issuance of counterfeit documents
- Provides mechanism to verify authenticity of paper based and electronic document by both the user to whom the document is issued as well as the organization that want to valid the authenticity of the document
- Provides mechanism to check integrity of content on the document
- Provides legal sanctity to electronic documents
- Also takes of tagging the document to the issuing authority

In conclusion, the proposed solution facilities the verification of a document both in its electronic as well as paper form. The solution is not only cost effective but also helps organization to issue documents/certificates to their citizen or customers without any hassle of verifying it later. The solution will help individual or organization to verify the authenticity of the document real time and does not require any manual intervention. Thus completely eliminating the creation of fake documents.

ABOUT THE AUTHOR

Sai Prasad brings 14 years of experience in the information security domain & also contributed to product innovation in PKI. Sai is also working towards acceptance and adoption of digital signatures in various industries & businesses.