

Secure 12N QR Framework Senior Project

Jacob Powell

Presented to the Management Department Faculty
of Oregon Institute of Technology
in Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Cybersecurity

Senior Project	2
Project Overview	3
Assumptions	6
Scope Statement	6
Impact Analysis	7
High-Level Risks	7
Milestones	8
Stakeholders	9
Roles and Responsibilities	9
Resources	10
Project Management Approach	11
Gantt Chart	11
Work Breakdown Structure (WBS)	13
Risk Management Plan	15
Activity Diagram	16
User Interface Design	16
Enhanced Entity Relational Diagrams	18
Application Development	18
Application Functionality	21
System Test Plan & Results	23
Future Developments	27
Acknowledgements	28

Project Overview

Introduction

Scannable media is becoming increasingly useful in today's digitally-intertwined marketplaces and organizations. Utilizing physical media to direct online interactions allows organizations to create accessible content portals for the public. This capability will only continue growing in value as more devices become internet connected, and cameras more prevalent. Invented in 1994 by the Denso Wave corporation, the current ISO/IEC DIS 18004:2023 QR standard is an evolution of the original concept for two-dimensional barcodes. The aim of this project is to introduce security controls for QR scannable media, by utilizing the updated 12N QR standard's security features and enhanced data capabilities.

Problem Identification

The identified issue which this project aims to resolve is an inherent vulnerability within the current ISO/IEC DIS QR standard. The vulnerability lies in the physical nature of pasted codes, which are susceptible to attackers physically pasting malicious or fraudulent media over legitimate scannable media. Users are particularly vulnerable to this attack vector due to the opaque nature of QR codes embedded media. This attack vector has been identified as problematic and actively exploited for over a decade, while still being identified by the FBI as a source of fraud as recently as 2021 (FBI Portland, 2021; A. Zimmerman, WSJ, 2006). During review of the Journal of Information Systems Applied Research, an article titled "QR Code Hacking - Detecting Multiple Vulnerabilities in Android Scanning Software" details the following attack vector (Homan & Breese, 2023):

1. The hacker uses the correct QR code to access a restaurant's menu.
2. The menu is copied and duplicated on a different website.
3. A new QR code is created that directs the scanning software to the fake website.
4. The new QR code is pasted over the restaurant's QR code at the table.
5. The diner scans the QR code and sees the menu on the fake website.
6. The malicious site uses HTML, SQL, or data injection to infect the smartphone and download personal data like contacts, calendar events, email, etc.
7. The user orders their meal completely unaware that they have been phished

This attack vector exemplifies the type of fraud and phishing attacks that this project aims to prevent. This attack vectors significance is reinforced through the article “QR Code Security -- How Secure and Usable Apps Can Protect Users Against Malicious QR Codes” recommendations to scannable media developers, which proposes:

“the integration of digital signatures in the QR code standardization to verify the origin of a code check for modifications. The overall idea is to derive a checksum (e.g. SHA-512) and encode it together with the content. The checksum is stored at an online trusted authority. When decoding the QR code, the QR code reader uses the checksum to verify the originator of the code with the trusted authority. A color indication or any other graphical representation should then indicate if verification was successful. To include digital signatures, QR code readers should be adapted to verify and display the result to the user, similar to SSL. For protecting the user against malicious URLs, checking the validity of HTTPS certificates would be an easy-to- implement measure” (Krombholz et al., 2015).

In Ron Lembke’s (Chair of Reverse Logistics Association and inventor of 12N QR standard) research paper titled “Reducing Cybersecurity Vulnerabilities Through the Use of 12N QR Codes”, he states “for greater security, asymmetric public key encryption may be used on any or all of the data in a 12N code. Additionally, private key encryption may also be applied to any data in the 12N code. Thus 12N codes provide the user with the ability to provide literally any information they desire to their users in a very compact form, with any level of security and encryption that they desire” (Carnovale & Yenyurt, 2021). This promotes the 12N QR standard as a suitable platform for implementing scannable media security controls. During a private discussion with Ron Lembke and Ken Jacobsen (Chair & Co-Chair of RLA), they confirmed these suspicions.

Finally, current scannable media applications have not implemented similar or similarly comprehensive solutions to the identified vulnerability. Cybersecurity industry leaders like Sophos, Kaspersky, and Norton have developed their own secure scannable media applications, which only implement embedded URL scanning against private databases as additional controls (Sophos Mobile Security, 2023; Norton Community, 2019; Kaspersky, 2023). These systems lack the comprehensive approach which is necessary to resolve such an inherent vulnerability. Overall, a review of literature surrounding inherent vulnerabilities in scannable media concurs with my proposed solution and implementation of the 12N QR standard.

Proposed Solution

To protect against identified scannable media vulnerabilities, I propose implementing the solution recommended by Krombholz et al. within the newly developed 12N QR standard. The implementation would utilize the 12N standards variable and encrypted fields to host selected media and checksums for third party verification by an online trusted authority. These checksums contain information and certificates authenticating the scannable media and displaying business information to prospective users. Users who scan unsupported or unauthorized codes are warned beforehand, and provided increased information about the embedded URL. This solution aims to prevent users from accessing malicious or fraudulent sites unknowingly due to the aforementioned opaque nature of embedded QR media.

Project Benefits and Anticipated results

Multiple positive outcomes as a result of project development have already been identified, such as:

- **Enhanced Security:** By implementing the 12N QR standard with integrated security features, the project significantly reduces the risk of phishing and fraudulent activities through scannable media.
- **User Trust and Safety:** The secure scannable media standard assures users of the authenticity and safety of the QR codes they scan, fostering greater trust in digital transactions and interactions.
- **Innovation Leadership:** Adopting the latest standards in QR technology positions organizations as leaders in innovative and secure digital solutions.
- **Accessible Security:** Provides small-businesses who cannot afford enhanced security solutions which require greater investment than the print costs of QR codes.

Additional positive outcomes based on anticipated results have been identified as:

- **Reduced Incidence of Fraud:** A notable decrease in fraudulent activities related to QR code scanning.
- **Increased User Engagement:** Higher engagement rates due to improved trust in the security of scannable media.
- **Positive Brand Perception:** Enhanced brand reputation as a secure and user-friendly digital service provider.

Assumptions

List of Assumptions for project feasibility:

- **User Compliance:** Users will adopt the updated QR scanning practices.
- **Technical Feasibility:** The 12N QR standard can be integrated seamlessly into existing systems.
- **Regulatory Approval:** The solution will comply with relevant data protection and privacy regulations.
- **Development in 12N QR Attack Vectors:** The solution will not be rendered ineffective by an unknown vulnerability in the 12N standard.
- **Application Security:** The solution will be applied via new application development which will integrate already developed application security standards

Scope Statement

Project Objectives:

1. **Development of 12N QR Standard Integration:** This involves creating and implementing methods to integrate the new 12N QR standard into existing systems for use within authentication. This standard offers enhanced security features and encryption capabilities, which are vital for the project's aim to improve scannable media security.
2. **Development of Application and User Interface Enhancements for QR Code Scanning:** The project will involve creating or updating applications with user interface improvements specifically designed for scanning and interacting with the new 12N QR codes. This will ensure ease of use and accessibility for users.
3. **Development of QR Media Security Feature Implementation:** The project will focus on incorporating security features as recommended by industry experts into the 12N QR codes. This includes embedding digital signatures, checksums, and possibly integrating encryption methods to authenticate and verify the QR code's source and integrity.

Exclusions:

1. **Non-QR Code-Based Scannable Media:** The project will solely focus on QR code-based media. Other forms of scannable media, such as barcodes or RFID tags, are not within the scope of this project.
2. **Backwards Compatibility with Older QR Standards:** The project will not prioritize making the new system compatible with older QR standards. The emphasis is on leveraging the advanced features of the 12N QR standard, which may not be compatible with older technologies.
3. **Physical Hardware Upgrades for Scanning Devices:** The project does not include upgrading the physical hardware of scanning devices. The focus is on the software and standard implementation, assuming that current devices are capable of scanning the updated QR codes.

Summary:

The project is focused on enhancing the security and reliability of QR code-based scannable media using the 12N QR standard. The aim is to utilize and potentially modify the 12N QR standard, by implementing it into a phone application which can produce and scan the modified 12N codes. These codes will contain information that is verified by a third party authenticator server, which will also need to be developed. Overall, the project represents a substantial but manageable time-investment, with clear project objectives and exclusions.

Impact Analysis

The project will not impact our sponsors' existing systems or processes. The project will be executed independent of any outside actors, or individuals. It will not be accessed by any who are not project sponsors or technical advisors. The project's created systems will be an application, backend authentication server, and any physically printed QR codes. No existing systems will be modified. Due to this, all materials can be secured from the internet and other outside observers.

High-Level Risks

- **Technology Adoption:** Users may be hesitant to transition to a new standard, especially if they are accustomed to the current QR systems. Overcoming this requires comprehensive user education and marketing strategies to demonstrate the enhanced security and benefits of the new standard. Additionally, ensuring the new system's ease of use will be

crucial for encouraging adoption.

- **Integration Challenges:** Integrating the 12N standard with existing systems presents technical hurdles. The challenge lies in ensuring that the new standard is compatible with a wide range of devices and platforms, both old and new. This requires meticulous planning, extensive testing, and possibly the development of bridging technologies to ensure smooth integration. Collaboration with device manufacturers and software developers will be critical to address these challenges effectively.
- **Regulatory Compliance:** With the rapid evolution of digital security laws and privacy regulations, ensuring that the solution remains compliant can be challenging. This risk is heightened by differing regulations across regions and industries. Staying informed about current and upcoming regulations, and building a flexible system that can adapt to regulatory changes, is essential. Engaging with legal experts and regulatory bodies during the development process can help in navigating these complexities.
- **Malicious Authenticators:** The risk of malicious entities posing as authenticators or compromising the authentication process is significant, especially given the reliance on third-party verification in the proposed solution. To mitigate this risk, establishing a robust verification process for authenticators is essential. This might include multi-factor authentication, continuous monitoring for anomalous activities, and regular security audits. Collaborating with established, reputable authentication service providers can also help minimize this risk.

Milestones

- **Development of 12N Standard Integration**
 - **Initial Planning and Design:** Define project scope, gather requirements, and finalize the design for integrating the 12N QR standard.
 - **Development Phase:** Start the coding and development of the 12N QR standard integration. This phase includes developing the necessary algorithms, encryption methods, and other technical aspects.
 - **Internal Testing and Iteration:** Conduct internal testing of the developed integration. Identify and rectify bugs or issues.
 - **Finalization and Review:** Finalize the development based on feedback and prepare for the integration with the user interface.

Stakeholders

Project stakeholders include:

- Gary Lomprey (Project Sponsor + Faculty advisor)
- Jacob Powell (Student / Project Manager)
- Reverse Logistics Association (Technical Advisors)

Roles and Responsibilities

Project Team: Jacob Powell (Student / Project Manager)

Role: Lead and coordinate the project, ensure milestones are met.

Responsibilities:

- Oversee project development and execution.
- Coordinate between team members and stakeholders.
- Manage project timeline and resources.
- Ensure the project adheres to technical and regulatory standards.

Stakeholder: Gary Lomprey (Project Sponsor + Faculty advisor)

Role: Provide guidance, resources, and decision-making support.

Responsibilities:

- Facilitate project funding and resources.
- Offer expertise and advice.
- Review and approve project milestones and deliverables.

External Parties: Reverse Logistics Association

Role: 12N QR Technical advisors

Responsibilities:

- Provide feedback on the usability and functionality of the system.
- Provide light detail on 12N QR code integration and history
- Final approval of

Resources

No external resources are required for this project. Due to the nature of the implementation, all work is to be completed in software development and deployment across already owned hardware. Due to the proof-of-concept nature of the application, the limited development will be completed utilizing pre-owned hardware.

Project Success Metrics

Below is a project success metric matrix which outlines the project success metrics targets, and acceptable score ranges:

Metric Category	Metric	Target	Scores
Stakeholder Satisfaction	Feedback and satisfaction scores from stakeholders	Average rating of 4 out of 5 or higher in feedback forms	4/5 average satisfaction rating
Technical Achievement and Completion	Completion of Development Milestones	Achieve all scheduled milestones within the designated project timeline	Completed 8/8 milestones within the timeline
Compliance with 12N Standards	Adherence to 12N QR Format Specifications	Full adherence to the technical and security specifications of the 12N QR standard	Achieved 100% adherence to 12N specifications
Integration Success with Existing Systems	Successful 12N QR standard integration	Successful integration within a set period	Integrated in 4 months
Innovation and Leadership in the Market	Recognition or references in industry publications, adoption by industry leaders	Achieve at least one form of industry recognition within the first two years	Received at least one industry publication

Project Management Approach

Upon initial project approval, development plans were created to reflect an iterative software development cycle. The core of my project relies on translating the 12N QR standard into an application, and then applying my concept to said application. The selected approach aimed to create the foundational core of the application this term, for completion in the following term. This foundational core has been identified as the core 12N scanning, creation, and encryption / decryption tools. These tools compromise the core of the project and post creation that conceptual side of the project can be implemented quickly. To create an outline of this term's iterative development goals, I discussed and selected three software goals to establish this foundational tech core:

1. Develop 12N QR code decryption algorithm, which can be used with 12N QR code decoding tools
2. Develop 12N QR code encryption algorithm, which can be used with 12N QR encoding tools
3. Develop 12N QR code certificate based encryption / decryption processes, which can be used with a certificate management server for secure information storage

Representative of these outlined goals, the development timeline for this term was divided into three, three week long development periods, focused on their respective goals. In addition, one week would be reserved for initial project planning and development. This initial week would be used to select development platforms, programming languages, and related packages to implement for project development. Overall, all of the outlined goals were achieved.

Gantt Chart

The below Gantt Chart Timeline and Duration charts represents the timeline of project development with detail on each week's completed development goals:

(On Next Page)

Week	Task Name	Description	Duration (Hours)
1/16/24	Initial Planning and Rapid Design	Scope definition, requirement gathering, design drafting.	19
1/23/24	Intensive Development of 12N Integration	Development environment setup, core algorithm coding, encryption method development.	21
1/30/24	Intensive Development of 12N Integration Continued	Continued	26
2/6/24	Phone App Core Development Completed	Core Features (12N creation, decoding, scanning) functional on app	19
2/13/24	Phone App Initial Certificate Implementation Testing	Conduct comprehensive integration testing to ensure the core features (12N creation, decoding, scanning) function seamlessly together.	16
2/20/24	Phone App Certificate Initial Implementation, Debugging	Implement initial certification methods, structuring, and refactoring for bugs. Implemented a thumbprint based certificate ID system.	16
2/21/24	Phone App Keystore & Certificate Encryption / Decryption Implementation	Focus on debugging the initial certificate implementation based on feedback from testing. Implement Android Keystore to handle certificate data.	20
3/6/24 BREAK	Phone App Certificate Handling Rewrite for Private / Public Key Management	Initial Implementation was unsuccessful due to unknown requirements of android keystore certificate keys. Rewrite of certificate integration.	22
3/27/24	Phone App Rewrite Start for Xamarin Depreciation	Xamarin officially depreciated causing all Xamarin apps to be non-functional post May 2024. Port from Xamarin to traditional C# Android application required.	45
4/3/24	Phone App Rewrite Complete	Completed Rewrite.	18
4/10/24	Phone App Encryption / Decryption Implementation	Post transition to a standard C# platform, the encryption and decryption mechanism was implemented throughout the application, requiring considerable rewrites.	24
4/16/24	Phone App Database Implementation	The database then had to be introduced to confirm authenticity of provided codes	16
4/23/24	Phone App Finalization / Translation to Paper	Finalizing application, adding comments, cleaning code to only show useful methods for future developers.	36
5/24/24	Project Paper, Poster, and Article Development and Finalization	Developed and finalized a project paper, Ideafest poster, and article by adding details, creating a poster, drafting an article, and reviewing all components to meet standards.	60
Total Hours:			352

The above provided Gantt Chart breaks down the timeline of software development, with the Xamarin rewrite representing the significant setback causing timeline delays. In addition, weekly goals had been set within the overall term goals scope, representing a weekly breakdown of required work.

Work Breakdown Structure (WBS)

1. Project Planning and Design

- Estimated Hours: 20
- Period: 1/16/24 - 1/22/24
- Potential Activities:
 - Define project scope
 - Gather initial requirements
 - Draft preliminary designs

2. Core Development and Implementation

- **2.1 Development of 12N Integration**
 - Estimated Hours: 50
 - Period: 1/23/24 - 2/5/24
 - Potential Activities:
 - Set up development environment
 - Begin coding core algorithms & encryption
- **2.2 Phone App Core Development**
 - Estimated Hours: 20
 - Start Date: 2/6/24
 - Potential Activities:
 - Develop foundational app functionalities such as 12N creation, decoding, and scanning

3. Testing and Debugging

- **3.1 Testing and Initial Debugging**
 - Estimated Hours: 40
 - Period: 2/13/24 - 2/21/24
 - Potential Activities:
 - Conduct integration and functionality testing

- Explore initial certification and debugging methods

- **3.2 Encryption and Key Management**

- Estimated Hours: 45
- Period: 2/22/24 - 3/5/24
- Potential Activities:
 - Implement encryption solutions and debug
 - Plan and potentially revise key management systems

- 4. **Platform Transition and Enhancement**

- Estimated Hours: 70
- Period: 3/6/24 - 4/9/24
- Potential Activities:
 - Assess and execute the transition from Xamarin to a C# Android application
 - Reimplement encryption/decryption mechanisms as required

- 5. **Finalization and Documentation**

- Estimated Hours: 55
- Period: 4/10/24 - 4/24/24
- Potential Activities:
 - Implement a database system for code authenticity
 - Finalize the application, ensuring readiness for future development and documentation

Total Estimated Project Hours: 300 Hours

The created work breakdown structure represents a rough outline of planned development activities. Each section is part of the outlined goals, with steps representing rough development required to achieve each goal. Each of these goals is a rough approximation of development requirements, with iterative development processes taking place at each step (testing, debugging, rewrites, etc). In addition, provided, the work breakdown structure and Gantt chart do not represent significant outside time investment into research and development of underlying technical concepts. These concepts include but are not limited to: ZXing library implementation, Android SDK implementation, Android emulation debugging, etc.

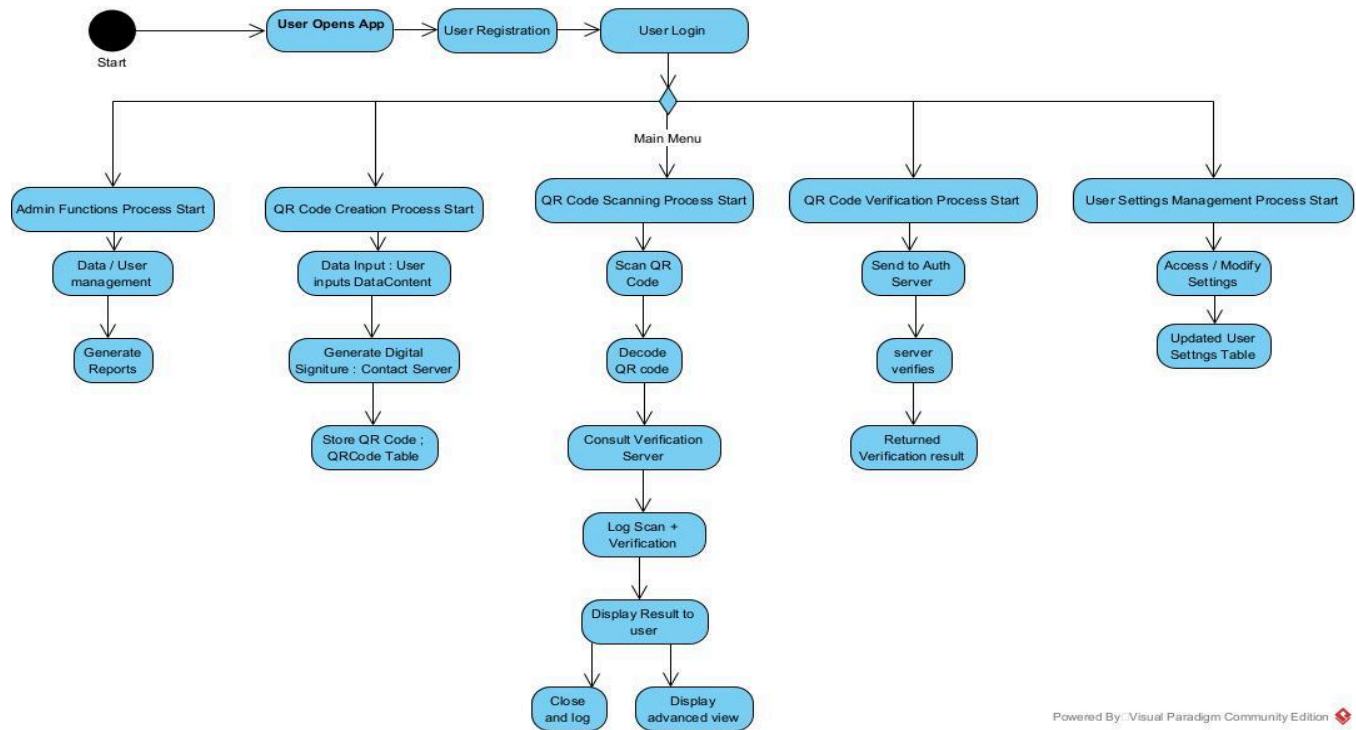
Risk Management Plan

Risk Management Matrix		
Risk Category	Description	Mitigation Strategies
Development Delays	The project may experience delays due to unforeseen technical challenges or resource constraints.	Implement agile project management methodologies to allow for flexibility in planning and execution. Prioritize tasks based on importance and urgency.
Technical Integration	Integrating the new 12N QR standard with existing systems and platforms may encounter compatibility issues.	Conduct early and continuous testing with existing platforms. Establish a technical working group to address integration challenges.
Compliance & Security	Ensuring the project complies with the latest security standards and regulations, which may evolve over the project's lifecycle.	Engage with cybersecurity experts and legal advisors to ensure ongoing compliance. Incorporate security by design principles throughout the development process.
Technology Obsolescence	The rapid pace of technological change may render the developed system or parts of it obsolete before it delivers the expected benefits.	Adopt modular design principles to facilitate easy updates and replacements. Monitor technological trends and plan for incremental updates to keep the system relevant.
Resource Allocation	Inadequate allocation of resources (time, budget, personnel) could impact the quality and timely delivery of the project.	Develop a detailed project plan with clear resource allocation. Regularly review project progress and adjust resources as needed to address any shortfalls or bottlenecks.
External Dependencies	The project's success may depend on external partners or technology providers, whose delays or failures could impact project timelines and quality.	Establish strong partnerships and agreements with clear expectations and contingencies. Diversify dependencies where possible to mitigate risks.

The above Risk Management Matrix represents a variety of potential project development risks and associated mitigation strategies. These risks are emblematic of the type of project development taking place, and the appropriate strategies for ensuring acceptable project timelines despite any encountered risks. Of these risks, development delays had occurred during project development, and a transition to an agile development plan had assisted in maintaining course. This change in development style led to more fluid additions and modifications to the code-base, leading to faster integration of problematic technologies.

Activity Diagram

Using the outlined project objectives, a basic phone application activity diagram was created to reflect app usage. The activity diagram outlines use-cases and normal user click-paths, helping outline database and user-interface design needs, for a finalized application:



User Interface Design

Using the outlined project objectives, a series of basic UI/UX example screens were developed to represent the completed applications information displays. These displays will be used to drive development and assist in visualization of project goals. These displays will be followed as a basic template for development of features, and provide project stakeholders visualizations of described current and future application development goals.

(Images Below)

Main Menu

12N Secure QR Application

Username

Password

Login

Exit

Create Secure QR Code

Scan Secure QR Code

User Settings

Admin

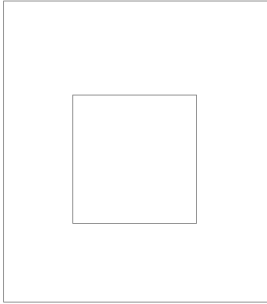
Secure QR Creation

Enter Link Address

Create Secure QR

Secure QR Scanner

Place QR in Center of Camera

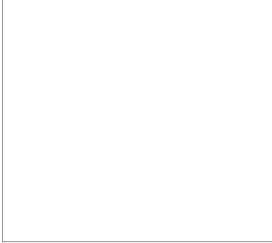


Scan QR

Valid Secure QR Link

Link Address

Website Preview



Additional Information

Open Link

Invalid unSecure QR Link

Link Address

Website Preview




Additional Information

WARNING: INVALID


Are you sure? Open Link

Admin Settings


Usertokens List



App Data



QR history



ETC

User Settings

Account Authenticator Token

Update Token

Username Change

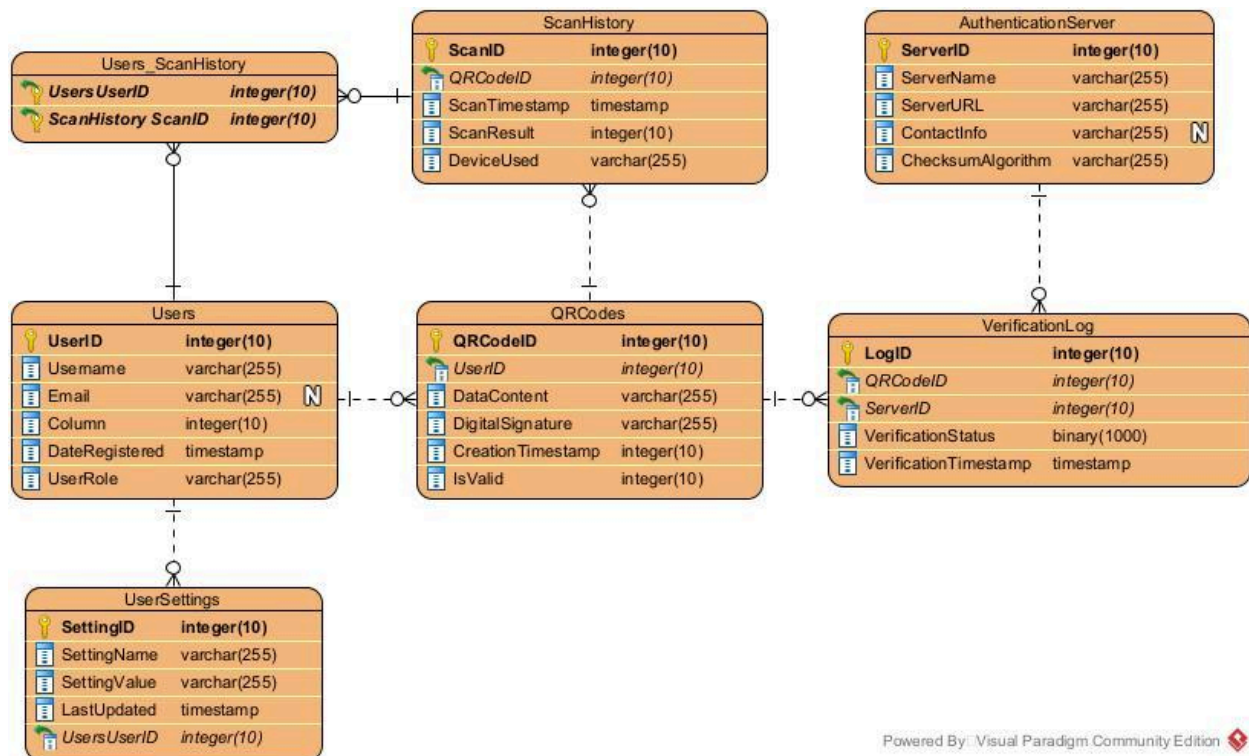
Update Username

Password Change

Update Password

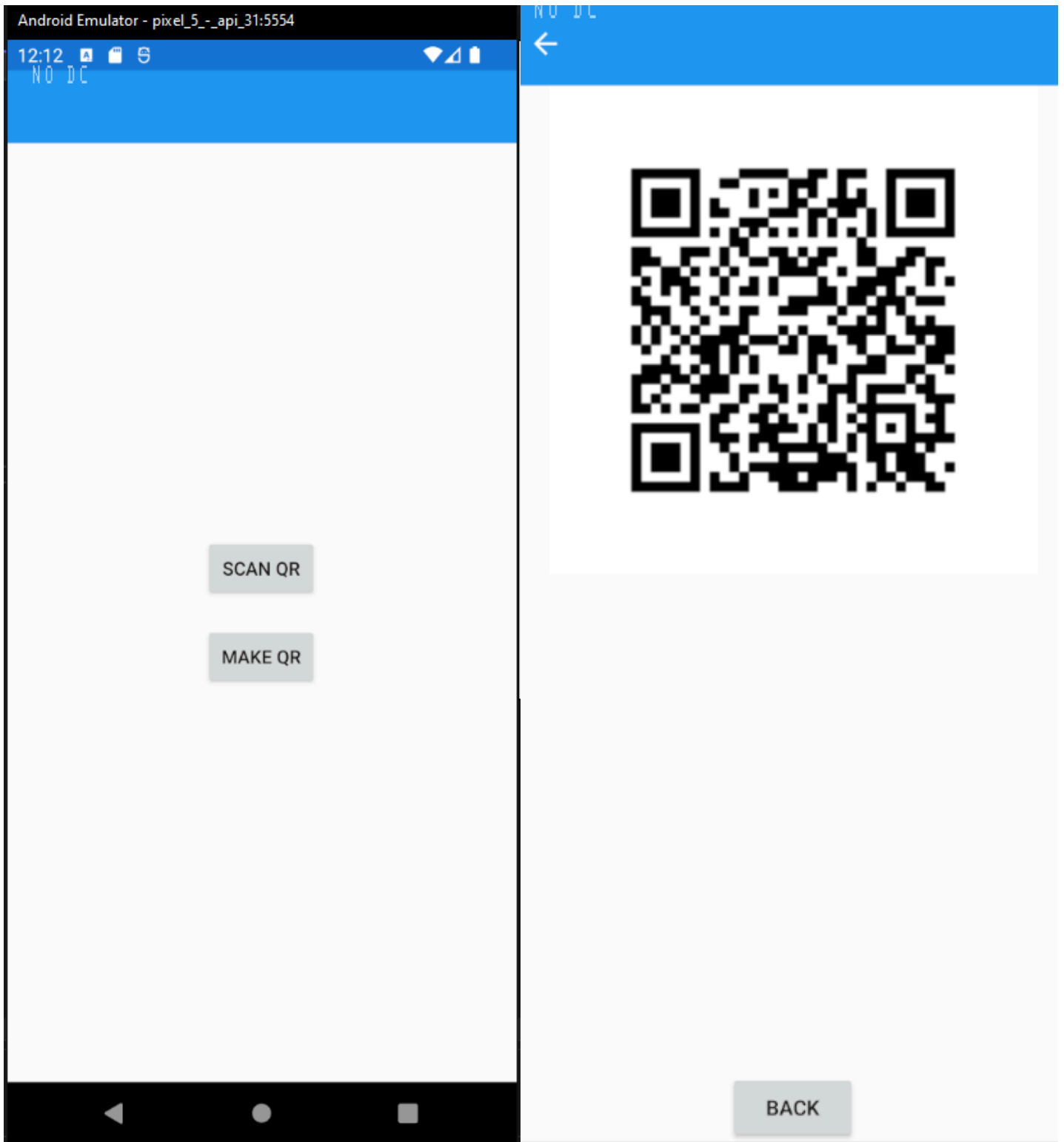
Enhanced Entity Relational Diagrams

Using the described project goals and user-interface outlines, an example enhanced entity relationship diagram was created to assist with database referencing programming. These tables are representative of the stored data needs of the application once moved to a server-based implementation. Currently, the program stores data locally, however the phone application has been designed to allow for fast transition to a server-based authentication system. The aim is to provide a framework for future developers to implement a 3rd party authentication server, below is the outlined ERD:

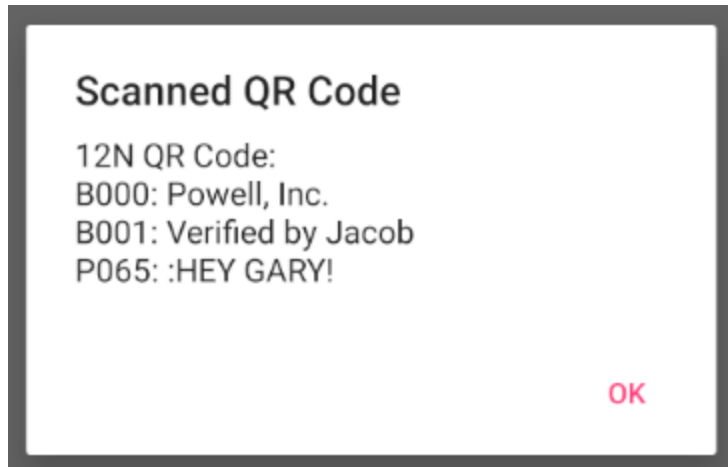


Application Development

The above documents represent the pre-code design required to support the projects' development moving forward. However, these designs represent only a fraction of the total time investment throughout the term, the majority of which was spent on software design and development for the phone application. This phone application represents a majority of the project's development goals, and as such was identified as a development priority. Below are screenshots of completed application developments (12N QR scanning, creation) as well as details on application development progress.



(Main Menu and Generated QR Code)



(Scanned 12N QR Code Decoded Data)



(12N Emulated QR Scanning Environment)

As seen in the provided images, the application successfully scans and generates 12N QR codes. While a simple functionality of standard QR scanning applications, these images are representative of significant work in 12N QR detection and decryption. Once published, the underlying code to decrypt and utilize 12N QR codes will be the only publicly available implementation in the world (no other authors have provided 12N QR code decoding / encoding platforms publicly, to my knowledge). In addition, generated 12N QR fields appropriately utilize

12N QR field names and data types, which are correctly recognized and decrypted by scanning algorithms.

Beyond scanning and QR creation, certificate based encryption methods were also implemented, with considerably less success. The initial implementation did not utilize Android Keystore, and attempted to manage and handle certificates directly without security measures. While an inherently insecure solution, it is acceptable for our test case pre-deployment. However, after multiple weeks of development, a major rewrite of said system was required to implement Android Keystore features.

Following the implementation of Android Keystore features and successful encryption / decryption methods, a major rewrite to port to a non-Xamarin platform was required. Xamarin, an open-source platform for building mobile applications was officially depreciated on May 1, 2024 (<https://dotnet.microsoft.com/en-us/platform/support/policy/xamarin>). This was unexpected, as no warnings about an upcoming depreciation were displayed when researching the platform. Due to this, a port to a standard Visual Studio C# Android platform was required. This port was a major rewrite, removing all use of Xamarin references while retaining core class functionality and methods.

The certificate and Xamarin rewrites represent the largest time investments and project roadblocks. Following these rewrites, the proof-of-concept application database was implemented to hold an example encrypted code for authentication in a local SQLite database. After successfully implementing the authentication database, a major rewrite was required to then finalize code and debug for enhanced functionality. Currently, the application is capable of handling standard QR codes, standard 12N QR codes, and encrypted 12N QR codes as required for conceptual implementation.

Application Functionality

Below is a step-by-step walkthrough of key application functionality in context of each pertinent class. In addition, the codebase for the project has been publicly shared for review and future development on [GitHub](#) aswell (Powell, 2024).

1. Application Initialization (MainActivity)

- QR Scanner Initialization: Utilizes the ZXing library for QR code scanning and generation.
- UI Setup: Initializes UI elements like buttons (scanQRButton and makeQRButton) and an ImageView (qrImage) for displaying QR codes.
- Event Handlers: Sets up event handlers for the buttons. The scanQRButton triggers the QR scanning process, while the makeQRButton checks if a certificate exists and, if so, generates a QR code using the loaded certificate for encryption.

2. Certificate Management (**CertificateGenerator**)

- Generate and Store Certificate: If no existing certificate is available, it creates a new RSA key pair and a self-signed X509 certificate, storing these in the PEM format in a specified directory.
- Load Certificate: Loads an X509 certificate from a specified file path, used for encryption or decryption processes.

3. QR Code Scanning and Processing (**QRScanner**)

- Scan QR Code: Requests camera permissions if necessary and scans QR codes using the ZXing library.
- Process Scan Result: Depending on the QR code's content, it either decrypts encrypted data or parses it according to the 12N standard, managing special formatting and separators as specified.

4. Encryption and Decryption (**CryptoUtils**)

- Encrypt Data: Uses RSA public key encryption for securing sensitive information within QR codes.
- Decrypt Data: Uses the RSA private key to retrieve original information from encrypted QR codes.

5. QR Code Generation (**QRGenerator**)

- Generate Encrypted QR Code: Encrypts specific fields using the public key from the loaded certificate and embeds them into a QR code, adhering to the 12N standard. Generates both an encrypted and a plain text version for verification.

6. Database Management (**DatabaseHelper**)

- Database Operations: Manages a SQLite database to store and verify codes that might be part of the QR code data, supporting operations like insert and query to maintain a list of trusted or known QR codes.

7. 12N Compliance

- Header and Trailer Management: Ensures each 12N tag starts with a required header and ends with a trailer as per the 12N specification.
- Special Character Usage: Handles unprintable characters (RS, GS, EOT, US) crucial for 12N compliance, ensuring proper format and parsing of the 12N data.

8. Key Functional Flows

- Starting the Application: Initializes the UI and sets up components when the app launches.

- Generating a QR Code: The user can generate a QR code by clicking the "Make QR" button. The app checks for an existing certificate or creates a new one, then encrypts data and displays the resulting QR code.
- Scanning a QR Code: By pressing the "Scan QR" button, the user can scan a QR code. The app processes the content, decrypting it if necessary, authenticates against the database, and displays the results.

Overall, this development represents a substantial benefit to the 12N development and research community as well as a demonstration of my concept. Specifically, the 12N QR scanning compliance and implementation of the technical guidelines as the first publicly shared development of this type in the space. Because of this, I believe future development utilizing the 12N QR standard, could find my contributions as a key source when beginning development.

System Test Plan & Results

Below is an annotated read out of the application's system test debug prints, which are triggered as methods succeed or fail to complete objectives. The following system test read-out is representative of the current application's functionality and ability to demonstrate the 12N 2FA QR framework. All objectives were completed as outlined, with the application successfully generating encrypted 12N QR codes with authentication data fields and scanning, decoding, and decrypting 3rd party 12N QR codes and generated encrypted 12N QR codes. The scanned encrypted data successfully decrypts using generated certificates and authenticates against the example internal database.

Example 3rd party 12N QR code (provided by Bruce Brown) scanned:

ZXing library is used to detect QR codes within bounds on camera launch:

1. [ZXing.Net.Mobile] Barcode Found

QR code is detected, unformatted data is extracted from QR bytes according to format:

2. QR Code scanned: []>0612NZ106:ZENVenUSDmCB000Powell, Inc.B001Verified by JacobP065... basic Text information, which I will check against my server's stored data

12N QR check method confirms 12N format before formatting for display:

3. Is12NQRCode check: True

Included 12N Data I requested for testing now formatted:

- 12N QR Code:106::
- ZENV: enUSDMC
- B000: Powell, Inc.
- B001: Verified by Jacob
- P065: ... basic Text information, which I will check against my server's stored data

Example full process encrypted 12N QR code + database entry generation:

Key Pair Generated:

Public Key:

-----BEGIN PUBLIC KEY-----

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmZj7aWlrOOK802wPqmE
qbnwQDNFGaRNOZjj3FIsQu3jdpbCBYTMMy7QmbI3+d/XA/BH1qB9rDQg6sg+Ry8j
y8La+PQtAzwiII/isCdrqvZKyLJC1Nz78L8y5keBX5oWWChYjVnh/A76yIFy+375
xU8s2LcRDwcdCabSVLX6FA94plRiZ4L8m2DPp39Jy50bVYrWdoW/FYCXqpykhjr3
L5X3QCQCp55dwJodCqsiw3laVrO3AiI2ZTwyd8WgdOCdDYRxxKVyH3ECEp2E4/sF
NhExpG519/KmiO2/ekbZ8O0uWmUFXGawfkz4asmAEuZvk+ueG+O+aeLoQ9ZnL4cW
RwIDAQAB
```

-----END PUBLIC KEY-----

Private Key:

-----BEGIN RSA PRIVATE KEY-----

```
MIIEowIBAAKCAQEAmZj7aWlrOOK802wPqmEqbnwQDNFGaRNOZjj3FIsQu3jdpbC
BYTMMy7QmbI3+d/XA/BH1qB9rDQg6sg+Ry8jy8La+PQtAzwiII/isCdrqvZKyLJC
1Nz78L8y5keBX5oWWChYjVnh/A76yIFy+375xU8s2LcRDwcdCabSVLX6FA94plRi
Z4L8m2DPp39Jy50bVYrWdoW/FYCXqpykhjr3L5X3QCQCp55dwJodCqsiw3laVrO3
AiI2ZTwyd8WgdOCdDYRxxKVyH3ECEp2E4/sFNhExpG519/KmiO2/ekbZ8O0uWmUF
XGawfkz4asmAEuZvk+ueG+O+aeLoQ9ZnL4cWRwIDAQABaoIBADGVVHZG/7NVp+OA
OUrwg/Y0NKPNY5AgJ4np4cwvdJ8ctcHL5s17mQKaiZsd0wFCNApaTvy7NJoiuNgm
OkmOnX3FaQjwuFuP/RV3CO3io09n8k5Tiu8I53BKWDaR53CygZb5/ottwX8tbalR
SLN7wbPZ6CXkwvsVH2qHdqlxhECiOS0nBIsDVvqntJnWeR4hPu9fFVZ1/DOJgN4t
oXANwXcwYmIaw7KeSGjCzqtVEXbcsr3DpnsBKSaOTVJE2ezLVekfEAHhD5IdtLZ
Eo0VjfQjAHofrXigGPR6cWxVlxwZkefNiVZHqsi8OjRRJG5Q0hOuKP2K0YNsOIO
iDUBfmkCgYEA5rAHKylVXzT8D0rFsUWrqQ85GYVQuytCtkOXiFMRAiplghVmNso
wWfJmSK0kvHqm6/SnR5QSt4mlVkrJlmhn22UBxuUf4e5DweRzMAMdBYDPk59f/NP
yWhIQHv89saCwI4NC+UYRm9czY2Aiz6VsGpM5ZXEhE5ay4IQeb7grQ8CgYEAtDgs
0Av1BwUweoNjJDS5AVJw+MQauMGlD9VfbQUnepf5Pj2oWuIjPX4CICpXY4iHHkSK
So5XjPIhVNDJ4EBR0OKSYtDOyNS97IWNXIVIO79XmDlvtXlsPJKNo//rH5Z9MLJC
tSIICoXZkP62IsUxQgTF4+6h35zLFNPGDIc0kCgYEAqZL2Ag1FO1log1k0j0Ym
lISjNZZhLOUH2mgrjxmNVptP5gDEYzOe9uTDNbVkraxdCAqr6GEzJoW8mQZOCmFU
Xexf5wWoGEL9jwXCcF8wCFlyEugBqv+BRAlLJ1O9NO3hi5lkP70tJgGQl20P88uS
n3bUheOc7KDobzXzwzDDZMCgYAVZDGVhEXStoBhmmTTMFrhWErGjGhrk7izT6Vj
CGCWQNw2UhVArbpHT0S5F4mF6/e1lQbhmKldvcPZaKL9tkS/2ZTsm8JfyjJKGh+
GetZOy4HiJHE5aO+UNrI13Ri
```

-----END RSA PRIVATE KEY-----

Certificate Information:

- Subject Name: CN=My Application

- Issuer Name: CN=My Application
- Serial Number: 195383110250047806521116936094860792363877
- Valid From: 5/2/2024 12:00:00 AM
- Valid Until: 5/2/2026 12:00:00 AM

Insecure local storage of test certificate data, to be done server side in future implementations:

1. Public Key stored at:
/storage/emulated/0/Android/data/com.companyname.App15/files/public_key.pem
2. Private Key stored at:
/storage/emulated/0/Android/data/com.companyname.App15/files/private_key.pem
3. Certificate stored at:
/storage/emulated/0/Android/data/com.companyname.App15/files/195383110250047806521116936094860792363877.pem
4. Certificate generated and stored successfully.

Certificate Data:

- Certificate Serial Number: 195383110250047806521116936094860792363877
- Using Certificate ID: 195383110250047806521116936094860792363877
- Pre-Encrypt Data: ABC123
- Pre-Encrypt Data: ExampleName
- Plain 12N Data: [>0612NP065:ABC123B000:ExampleName
- Encrypted 12N Data:
[>0612NZENC195383110250047806521116936094860792363877P065:RnTM5ToRRvMzKG
R6WBAsyFWBaxkxRNHlPs37Wr75JwVFA++ZLe50VeB5BZD+hT0Jwvh81qEmL8m+HGbgWWOI2d/4lqaN990WPfCMifVMtDxs
0BY2TBRkcL9z0BthNTb1o7jMC772MMNxPfnLFbICLf8OY0/WcENqyBEPR5g+PHoTMpYbyyn5Kjofvwt79wNUeus+FjkwW2B
58VHfpcbj4xfeYXsSn7nFFpWkB0tE4qeRHBraYPW15yyS3KiATxW2TII1CIB4qwUSikX7RNj5uvShKOUmkuExlUnmPij3bCGI7a
YiMdNKpr6C6DgZTDPFKjXR3ZrHQ1Uk5bHSTLPTQ==B000:ZgDDz0qm4OXZNa5pCd4ZruhSVvneCyYzVO1reL5R8BQH
9chBbGDkfvjCjhL+aAv865FT/sbWUYv8zteFejAL8jdDzzgW7rr675mfWaJBPGl8sZk26N2EFPJoxf3pb/XByjFn4bKli39CjGIWe8an
T7iRk/6DyyUSqeFGypG/oLWardUWW3+v1JZ6aIQuduzlvZhrTuQewHTtkpowFe7Nkgr1RZGznADSAkuy9WXUFylnqE7li8L+lxp
yBOqu+LpJfquxnCEGOxyhA22hRga3b9eJqeRpYRPA/BRJOrscnLd1KGI6KfGkN3g8KH8gkR5uiMTbsiEb5jkl6wGLRJ505w==

Scan + decryption process for encrypted generated 12N QR code:

1. QR Code scanned:
[>0612NZENC195383110250047806521116936094860792363877P065:RnTM5ToRRvMzKG
R6WBAsyFWBaxkxRNHlPs37Wr75JwVFA++ZLe50VeB5BZD+hT0Jwvh81qEmL8m+HGbgWWOI2d/4lqaN990WPfCMifVMtDxs
0BY2TBRkcL9z0BthNTb1o7jMC772MMNxPfnLFbICLf8OY0/WcENqyBEPR5g+PHoTMpYbyyn5Kjofvwt79wNUeus+FjkwW2B
58VHfpcbj4xfeYXsSn7nFFpWkB0tE4qeRHBraYPW15yyS3KiATxW2TII1CIB4qwUSikX7RNj5uvShKOUmkuExlUnmPij3bCGI7a
YiMdNKpr6C6DgZTDPFKjXR3ZrHQ1Uk5bHSTLPTQ==B000:ZgDDz0qm4OXZNa5pCd4ZruhSVvneCyYzVO1reL5R8BQH
9chBbGDkfvjCjhL+aAv865FT/sbWUYv8zteFejAL8jdDzzgW7rr675mfWaJBPGl8sZk26N2EFPJoxf3pb/XByjFn4bKli39CjGIWe8an

T7iRk/6DyyUSqeFGypG/oLWardUWW3+v1JZ6aIQuduzIvZhrTuQewHTtkpowFe7Nkgr1RZGznADSAkuy9WXUFylnqE7li8L+lxpyBOqu+LpJfqunCEGOxyhA22hRga3b9eJqeRpYRPA/BRJOrscnLd1KGI6KfGkN3g8KH8gkR5uiMTbsiEb5jkl6wGLRJ505w==

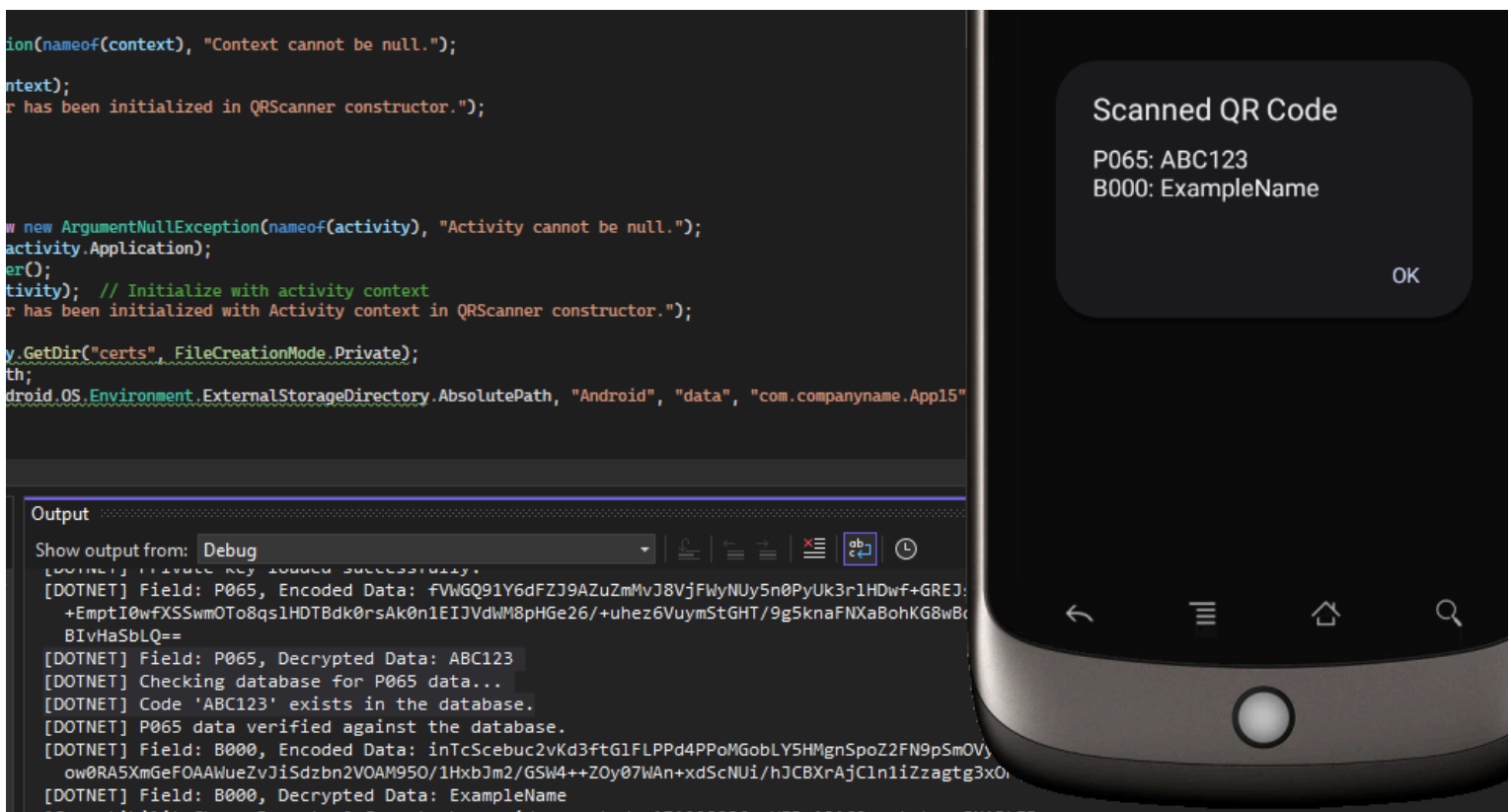
2. Starting decryption process...
3. Key read from file successfully.
4. Key is part of a key pair.
5. Private key loaded successfully.
6. Field: P065, Encoded Data:
RnTM5ToRRvMzKGR6WBAsyFWBaxkxRNHIPS37Wr75JwVFA++ZLe50VeB5BZD+hT0Jwvh81qEmL8m+HGbGWWOI2d/4lqaN990WPfCMifVMtDxs0BY2TBRkcL9z0BthNTb1o7jMC772MMNxFpmLFbICL8OY0/WcENqyBEPR5g+PHoTMpYbyyn5Kjofvwt79wNUeus+Fjkw2B58VHfpcbj4xfeYXsSn7nFFpWkB0tE4qeRHBraYPWl5yyS3KiATxW2TII1CIB4qwUSikX7RNj5uvShKOUmkuExlUnmPij3bCGI7aYiMdNkpr6C6DgZTDPFKjXR3ZrHQ1Uk5bHSTLPTQ==
7. Field: P065, Decrypted Data: ABC123
8. Checking database for P065 data...
9. Code 'ABC123' exists in the database.
10. P065 data verified against the database.

11. Field: B000, Encoded Data:

ZgDDz0qm4OXZNa5pCd4ZruhSVvneCyYzVO1reL5R8BQH9chBbGDkfvjCjhL+aAv865FT/sbWUYv8zteFejAL8jdDzzgW7rr675mfWaJBPL8sZk26N2EFPJoxf3pb/XByjFn4bKli39CjGIWe8anT7iRk/6DyyUSqeFGypG/oLWardUWW3+v1JZ6aIQuduzIvZhrTuQewHTtkpowFe7Nkgr1RZGznADSAkuy9WXUFylnqE7li8L+lxpyBOqu+LpJfqunCEGOxyhA22hRga3b9eJqeRpYRPA/BRJOrscnLd1KGI6KfGkN3g8KH8gkR5uiMTbsiEb5jkl6wGLRJ505w==

12. Field: B000, Decrypted Data: ExampleName

Below is an image detailing the decoded and decrypted, generated 12N codes information being displayed post-authentication against a database (an error is displayed if the database entry does not match the P065 code):



Overall, while the final scan result contains little information, the underlying process successfully integrates the 12N standard into a scannable media authentication service framework. While it currently remains a rudimentary implementation of both the 12N standard and the overall authentication capabilities, the developed application represents a substantial benefit to developers and researchers in both areas. The system test successfully demonstrates the completion of the technical achievement, compliance with 12N standards, and integration with existing systems project milestones. In addition, the system test confirms the 12N standard as a suitable platform for conceptual implementation of project solutions, and the viability of the 12N 2FA QR framework for future developments and integration.

Having shared my system test results and development progress with 12N Standard inventor Ron Lembke, I received positive feedback indicating my project met partner expectations. In our brief discussion, Mr. Lembke had indicated my suspicions regarding limited publicly available 12N QR applications and development resources (outside of published standards' information). In addition, Mr. Lembke had identified my developments as a solid implementation of the 12N standard within my concept, and as a promising development within the 12N community. Overall, representing a significant benefit to fellow junior 12N developers. Finally, RLA co-founder and project partner Ken Jacobsen has begun the article publication process within the Reverse-Logistics Magazine, with a planned project article submission meeting the project's innovation and publication metric. Overall, this represents a high level of project partner satisfaction and a confirmation of underlying conceptual assumptions regarding the suitability of the 12N standard.

Future Developments

While the current application represents a significant development in the public 12N QR scanning space, and demonstrates the concept successfully, there are still significant developments required before a public release or publishing. Some of the most important remaining developments are outlined below:

- Rework of 12N standard interpretation to better utilize available functionality and security features.

The current 12N standard interpretation successfully interprets generated and 3rd party 12N QR codes, however, the standard is extensive and a fully realized implementation of it may enhance functionality considerably.

- Implementation of 3rd party authentication server to securely host generated authentication and business data.

A 3rd party independent authentication server is required to fully implement the concept in a published release, as per the detailed proposed solution. This would be an extensive undertaking and require considerable resources to ensure consistency in uptime.

- Redesign of certificate based authentication to better utilize X509 certificate security functionality and create an independent trusted certificate authority server.

The development of a trusted certificate authority server with enhanced X509 certificate security system to better manage and control certificate authentication services.

- Complete redesign of application functionality to enhance security across all domains, such as database protections, management of encrypted data, and other relevant security functionality

The current application was developed as a proof of concept, and as such the current implementation is expected to be insecure and requires a comprehensive vulnerability review.

Acknowledgements

This project would not have been possible without the contributions of both my project partners at the Reverse Logistics Association (RLA Standards Committee Co-Chairs) and the support of Bruce Brown, founder of Informission Solutions Inc. In specific, I would like to acknowledge Ron Lembke, for both the excellent documentation provided regarding the 12N QR standard and project support; and Bruce Brown for providing a third-party 12N QR code for use in testing my system, and key advice related to its development. In addition, I would like to thank my family, as many times I had consulted my father Avi Powell in times of doubt and confusion. Finally, I would like to thank my project sponsor and faculty advisor Gary Lomprey for his continued support and guidance throughout my project's development and time studying at the Oregon Institute of Technology Portland Metro.

References

- 12N SQRL*. 12N code listing. (n.d.). <https://www.rla.org/page/sqrl-code-listing>
- FBI. (2021, October 19). *Oregon FBI Tech Tuesday: Building a digital defense against QR code scams*. FBI.
<https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/oregon-fbi-tech-tuesday-building-a-digital-defense-against-qr-code-scams>
- Gaydos, L. (2023, January 26). *Think before you scan – scammers can use QR codes to steal your information*. NBC Boston.
<https://www.nbcboston.com/news/local/think-before-you-scan-scammers-can-use-qr-codes-to-steal-your-information/2955087/>
- Homan, J., & Breese, J. (2023). QR Code Hacking – Detecting Multiple Vulnerabilities in Android Scanning Software. *Journal of Information Systems Applied Research*, 16(1), 13. ISCAP. Retrieved from <https://jisar.org/>; <https://iscap.info>
- Krombholz, K., Frühwirth, P., Kieseberg, P., Kapsalis, I., Huber, M., & Weippl, E. (1970, January 1). *QR code security: A survey of attacks and challenges for usable security*. SpringerLink. https://link.springer.com/chapter/10.1007/978-3-319-07620-1_8
- Microsoft. (n.d.). Xamarin official support policy: .NET.
<https://dotnet.microsoft.com/en-us/platform/support/policy/xamarin>
- Powell, J. (Apr. 27, 2024). 12N-2FA-QR-Project: Public filesource for 12N 2FA Secure QR Standard Senior Project. *Oregon Institute of Technology*. GitHub.
<https://github.com/JacobPowellCybSec/12N-2FA-QR-Project/tree/main>
- QR code scams are on the rise. here's how to avoid getting duped*. CNET. (n.d.).
<https://www.cnet.com/tech/services-and-software/qr-code-scams-are-on-the-rise-heres-how-to-avoid-getting-duped/>
- RLA Committee Standards*. RLA Standards Committee. (n.d.).
<https://rla.org/committee/standards>