جامعة الملك سعود
King Saud University

GP1
concealsafe

www.concealsafe.com

Group #24

Content

- Problem, Solution & roadmapOur Services 02
- Background & literature reviewStrategy 03
- System requirements Evaluation 04
- System DesignProjects 05
- System Testing 06
- Conclusion & Future Work 07
- 08

Problem:

Digital communication is under threat as cyberattacks grow more advanced. Traditional encryption protects the content but fails to hide its existence, often attracting malicious attention.

Without hidden protection, sensitive data becomes an easy target. To stay secure, we need more than encryption—combining it with steganography is essential to keep our data safe and unnoticed.

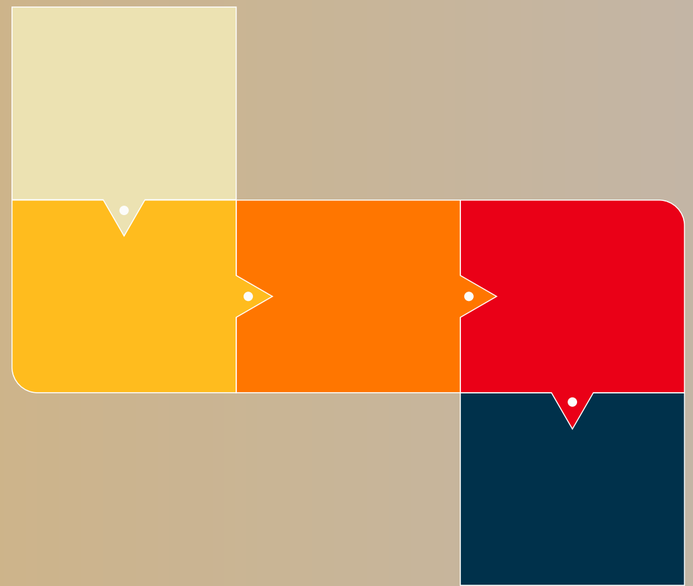
Solution

To tackle modern data security challenges, our project combines cryptography with steganography in a comprehensive web application.

Key features include:

- **Encryption**
- **Steganography**
- **Multi-Factor Authentication**
- **Public Key Infrastructure (PKI)**
- **Diverse Data Handling**

ROADMAP



Roadmap

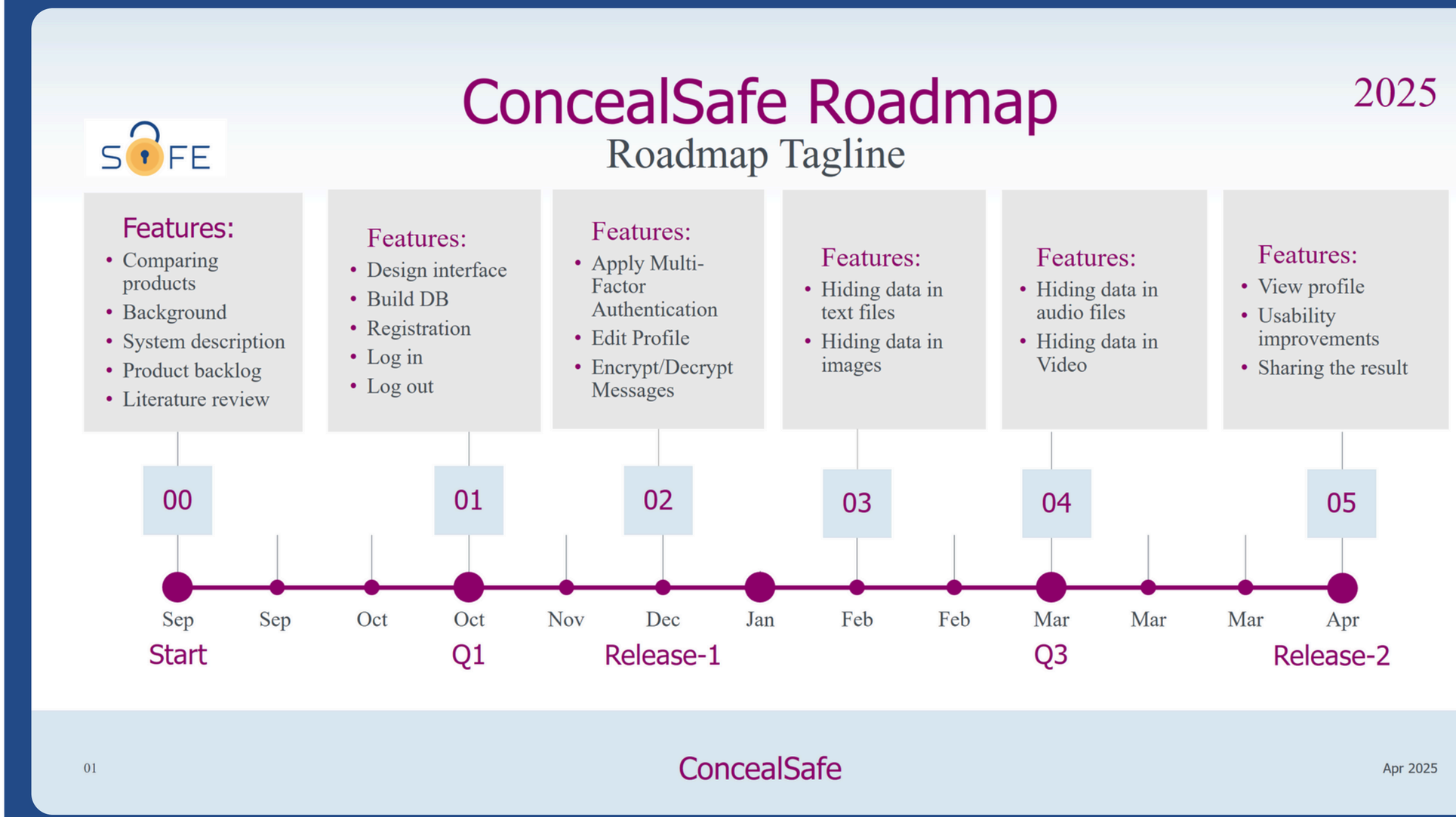


Figure 1 (Product roadmap)

BACKGROUND

Background: Encryption

- Converts readable data into an unreadable format.
- Protect and ensure the integrity of sensitive data.

Types of Encryption:

- Symmetric: Same key for encryption and decryption. E.g:(AES)
- Asymmetric: Uses public and private keys for secure exchange. E.g:(RSA)

Background: Steganography

- Hides data within other media (e.g., images, audio) to conceal its existence.
- It keeps the communication more secure.

Background: Multi-Factor Authentication

- Authentication using two or more verification methods
- Reduce brute force attacks and ensures secure access.

The types of MFA include:

- Something You Know: Passwords, PINs.
- Something You Have: OTPs, smart cards.
- Something You Are: Biometrics (e.g., fingerprints).

Background: Public Key Infrastructure (PKI)

- A framework using digital certificates for secure communication.
- Use a public Key for encryption, and a private key for decryption.
- Authenticates users and devices. and Secure message sharing.

Background: Application Programming Interface (API)

- API is a set of tools and protocols that allows different software applications to communicate and share data or services with each other.

APIs used in this project:

- Cryptogrophy API for Encryption/Decryption and issuing certificates for PKI
- Steganography API, the Least Significant Bit (LSB)
- File Upload and Management API