# Electronic Resident Identity Card

Elend Venture, Gyorn Hrathen

University of Svorden

**Abstract.** The electronic Resident Identity Card (e-ID) system proposes a modern and secure method for identity verification, leveraging the capabilities of mobile devices. This paper outlines the design and implementation of an e-ID system, focusing on the efficient and secure issuance and presentation of the digital identity card. The system incorporates strong encryption, biometric authentication, and robust security measures to ensure data integrity and user privacy. We discuss the roles of the user, issuer, and relying party in the e-ID system, detailing the processes involved in issuing and verifying the e-ID. Additionally, we examine the technical and legal requirements necessary for the successful deployment of the e-ID, including revocation functionality to manage changes and threats effectively. Through this system, we aim to provide a seamless, secure, and user-friendly identity verification process that aligns with the needs of the digital age.

**Keywords:** digital identity · cryptography · security.

## 1 Introduction

In an increasingly digital age, the traditional physical identity card is evolving to meet the growing demands for convenience, security, and efficiency. The introduction of an electronic Resident Identity Card (e-ID) aims to streamline identity authentication processes, facilitate seamless access to various services, and enhance the overall user experience. This paper proposes a comprehensive solution for securely storing an electronic version of the resident's identity card on a mobile device, capable of being presented to relying parties (RP) for the identity verification.

The adoption of an e-ID brings numerous benefits. Firstly, it eliminates the need for physical ID cards, reducing the risk of loss or theft, and potentially making identity theft more difficult. Secondly, the ease of use and convenience afforded by mobile devices provide a more efficient verification method, particularly in high-traffic environments such as airports or border checkpoints. Lastly, an e-ID offers enhanced security measures that are critical in protecting personal information and preventing unauthorized access or use.

This paper outlines the architecture of the proposed system, emphasizing robust encryption technologies to ensure data confidentiality and integrity. Additionally, this paper provides an analysis of existing digital identity solutions and examines potential use cases for the e-ID, including government services, financial transactions, and travel authentication.

To achieve our goals, we focus on implementing a secure and efficient framework for storing the e-ID, ensuring compatibility with a wide range of mobile devices and existing infrastructure. We also explore the integration of this e-ID with existing identification systems to provide a seamless and trustworthy user experience.

In summary, this paper seeks to address the challenges of traditional identification methods while offering a modern, secure, and convenient solution for residents. By transitioning to electronic identity cards, we aim to enhance the overall functionality and security of identity verification processes in the digital age.

## 2 System

### 2.1 System components

The proposed electronic Resident Identity Card (e-ID) system consists of three main components: the user, the issuer, and the relying party (RP). Each of these components plays a crucial role in ensuring the secure and efficient use of the e-ID. Let us explain in the details of each component and its respective functions.

**User** is a party to whom e-ID is issued. User interacts with the system using Mobile Device. Users is required to download and install a secure application and engage in the issuing protocol to get e-ID. This application can be made available from a trusted repository (e.g., Google Play Store, Apple App Store). User must be able to present the e-ID to relying parties through mobile display on the device screen (physical presentation) or sending it as response to the authentication request from the relying party (online presentation).

**The issuer** is responsible for verifying the user's identity prior to issuing the e-ID. Once verified, the issuer generates a secure e-ID that is encrypted and stored securely. The issuer ensures that the generated e-ID is securely distributed to the user via a trusted and secure mechanism. The issuer adheres to all relevant laws and regulations regarding data protection, privacy, and cybersecurity. This includes maintaining strict confidentiality and ensuring that the e-ID can only be accessed by the rightful owner.

**The relying party** (RP) requests the presentation of the e-ID from the user to verify the user's identity. The relying party implements a secure and standardized verification protocol to validate the e-ID presented by the user. This ensures that the verification process is consistent and reliable. The relying party enforces robust security measures to prevent fraudulent presentations of the e-ID. This includes using tamper-proof technologies. The relying party maintains strict access controls to ensure that only authorized e-IDs can be used for authentication. This includes checking the validity and authenticity of the e-ID before granting access to protected resources. The relying party complies with all legal and regulatory requirements related to data privacy, identity verification, and information security. This ensures that the use of e-ID for authentication is trustworthy and secure.

### 2.2 System requirements

The proposed e-ID system should meet the following security requirements:

- The system must manage encryption keys and signing keys securely, including usage of Hardware Security Modules (HSMs) where applicable
- The e-ID data must be encrypted using strong, industry-standard encryption algorithms
- The system should rely on use of digital signatures to verify the authenticity of the e-ID data and to ensure that the data has not been tampered with
- The system must ensure that e-ID that was not created by the issuer does not pass verification by the RP
- The system must ensure post-quantum security for all the components
- The system must use standardised cryptographic algorithms
- The system must ensure that attackers getting access to the user's device are not able present honest user's credential to the RP
- The system must ensure strong user authentication before credential is issued
- The system must ensure that adversary cloning the mobile device memory, does not gain access to user' private information
- The system must ensure that adversary cloning the mobile device memory is not able to issue revocation, issuing and presentation requests (without active participation of user)

To keep the system lightweight on the user's mobile device and make issuing and presentation more efficient, we propose to send all the information over public communication channel. This helps to avoid overhead created by the TLS handshake and makes the protocol very efficient.

### 2.3 Protocols

The presented system consist of the following protocols – Issuing, Presentation, Revocation. The issuing protocol establishes a secure and verifiable process for generating and distributing e-IDs, incorporating strong encryption. The presentation protocol facilitates the secure and efficient presentation of the e-ID to relying parties. Finally, the revocation protocol provides a mechanism for promptly deactivating or invalidating e-IDs in response to security threats, changes in personal information, or other necessary actions.

Issuing Protocol:

1. User downloads and installs a secure e-ID application from a trusted repository (e.g., Google Play Store, Apple App Store).
2. e-ID application runs key generation to produce LUOV signature scheme key pair $(\mathsf{pk}_s, \mathsf{sk}_s)$.
3. User provides their personal information (name, date of birth, address, etc.) and uploads their photo.
4. e-ID application generates e-ID issuance request that contains user's freshly generated public key $\mathsf{pk}_s$, identification code $\mathsf{uid}$ and photo.

5. e-ID application sends issuance request to the issuer.
6. Issuer verifies the user's identity using photo provided in the request and comparing it to the one stored in the system (for the physical ID card).
7. Issuer generates the encrypted e-ID credential, which includes encrypted personal information, user identifier $\mathsf{uid}$ and user public key $\mathsf{pk}_s$.
8. Issuer sends encrypted e-ID credential to the user's device.
9. The mobile application decrypts all the fields in the received credential and stores the e-ID securely, by uploading it to the cloud.
10. The user receives a notification that the e-ID has been issued and is available in the app.

For the encryption of the e-ID credential by the issuer, we propose the system implementers to choose encryption scheme that suits their needs better. There is a variety of schemes to choose from (examples include DES, SHA3, AES, RSA-PSS, RC4 and ElGamal in OFB mode) and concrete choice depends on the system implementation and the efficiency requirements. For the signature schemes, we propose to use LUOV and ECDSA as both are well-known and well-studied signature schemes. The credential and encrypted credential are illustrated in 1.

After the key generation and issuing protocols, the user's device application stores the following information:

- LUOV signature key pair $(\mathsf{pk}, \mathsf{sk})$
- user identification code $\mathsf{uid}$
- user photo

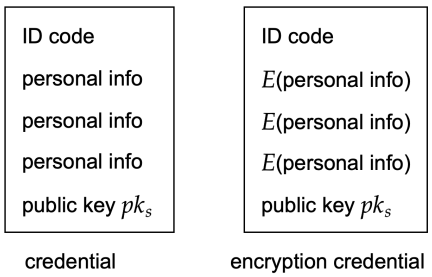


**Fig. 1.** Credential and encrypted credential. Each credential may contain many personal info fields. We do not restrict the number of field in the credential.

Presentation protocol (online presentation): User presents their e-ID to the RP. The RP has its ECDSA signature key pair $(\mathsf{pk}_r, \mathsf{sk}_r)$.

1. User wants to get authenticated to the services provided by the RP
2. User opens e-ID application and initiates the presentation process

3. Application retrieves e-ID from the cloud storage and creates presentation request to the RP, containing user identifier $\mathsf{uid}$.
4. Application sends presentation request to the RP.
5. RP sends the message to the application containing RP public key $\mathsf{pk}_r$ and signature on $\mathsf{uid}$ created as $\sigma = \mathsf{ECDSA.Sign}(\mathsf{sk}_r, \mathsf{uid})$.
6. Application verifies signature as $\mathsf{ECDSA.Verify}(\mathsf{pk}_r, \mathsf{uid}, \sigma)$.
7. If signature verifies, it sends e-ID to the RP.
8. RP verifies e-ID, by checking that all fields contain meaningful plaintext.
9. If e-ID verification is successful, user is authenticated.

### 2.4 Revocation functionality

The revocation functionality is crucial for the electronic Resident Identity Card (e-ID) system for several reasons. This feature ensures that the e-ID can be deactivated or invalidated when necessary, thereby maintaining the security and integrity of the system. Below, we bring some key reasons why revocation functionality is essential.

**Securing Against Unauthorized Use**. If a user's e-ID is lost or stolen, it becomes critical to revoke that e-ID to prevent unauthorized access or use. Without revocation, a stolen or lost e-ID could be used fraudulently, leading to security breaches and identity theft.

**Managing Changes in Personal Information**. When a user's personal information changes due to a name change, address update, or other life events, it may be necessary to revoke the old e-ID and issue a new one. Revocation allows for the timely and secure update of personal data, ensuring that the e-ID remains accurate and up-to-date.

**Addressing Security Vulnerabilities**. If a security vulnerability is discovered in the e-ID system, it may be necessary to revoke all active e-IDs to protect user data. Revocation enables prompt action to mitigate potential security risks, ensuring that the system remains secure and trustworthy.

**Maintaining Compliance with Regulatory Standards**. Regulatory bodies may require that e-IDs be revoked under certain conditions to comply with data protection and privacy laws. Ensuring compliance with legal standards through revocation functionality can prevent legal and regulatory issues, maintaining the trust and credibility of the system.

Revocation protocol:

We designed our system in such a way that the user does not need to communicate with anyone for the revocation process, since the user is in control of all the data needed to perform revocation. User may get notified by the issuer or authorities that their e-ID is not valid any more. After receiving this notification, user performs the following steps:

1. User opens e-ID application and initiates the revocation process
2. Application retrieves e-ID from the cloud storage
3. Application displays e-ID fields that the user can change (applicable when a user's personal information changes) and user performs needed changes.

This includes changing status of the credential (status is "valid" by default and can be changed to "revoked").
4. User confirms changes and application stores updated e-ID securely, by uploading it to the cloud.

Alternatively, the user may wish to modify or revoke credential themselves, which they can do without the need to communicate to any other parties.

## 3 Security

Since the system proposed in this paper uses well-known cryptographic primitives, we leave out the security proofs for the scheme as it they can be trivially derived from the existing literature.

## 4 Conclusion

The proposed electronic Resident Identity Card (e-ID) system offers a robust solution for identity verification in the digital age. By leveraging advanced security technologies, including encryption, and real-time verification protocols, the system ensures the integrity and privacy of user data. The roles of the user, issuer, and relying party are clearly defined to provide a seamless and user-friendly experience, while maintaining stringent security measures. The inclusion of revocation functionality allows for the effective management of e-IDs, addressing potential threats such as lost devices, changes in personal information, and identified security vulnerabilities.

This system not only enhances the convenience and efficiency of identity verification processes but also adheres to regulatory requirements, ensuring compliance with data protection laws. The successful implementation of the e-ID system would provide a secure, reliable, and user-centric approach to identity verification, fostering trust in digital transactions and services. Future work will focus on further optimizing the system's performance and scalability, ensuring it remains a dependable tool in the ongoing evolution of digital identity management.

Additionally, we note that setting the requirements for credential expiration is out of scope of this work. Additional care should be taken when setting up the proposed system to make sure that each issued credential has expiration date set and this date is verified by the relying party.