CRYPTOGRAPHIC ID AND E-VOTING SYSTEM FOR PAKISTAN

Research Paper

NAME: MUHAMMAD ASAD
ROLL NO.: B16158051
CLASS: BS (SE) 3RD YEAR SECTION-A

Table of Contents

Cryptographic ID and E-Voting System for Pakistan

Introduction

Cryptography is the study to establish secure communication, for example, on the internet when thousands of users could intercept your communication i.e. in the presence of third parties called adversaries. In this research paper we will be discussing, the possibility of electronic/digital ID cards that store identity information, encrypted and secure using cryptographic algorithms and can only be decrypted by official government organizations such as NADRA (in case of Pakistan). This will open huge opportunities to digitalize many aspects of government record keeping and can be used to create a very secure **Electronic Voting System** that Pakistan is in dire need of. In Pakistan, the election process is not secure or efficient and after each election, many accuse that the results are tempered with. This will be solved by the introduction of an e-voting system that will be much secure than the traditional system being used currently, with the added benefit of not calculating the results manually which is time-consuming and labor-intensive.

What are Cryptographic ID Cards?

Cryptographic ID Cards are simply ID Cards that store Identity Information in an encrypted format and the person/organization trying to access the information will require a key to decrypt it. This will ensure privacy. To verify, the encrypted information will be sent to the government organization, which has the key to decrypt, the encrypted information and verify it from their local database. Before understanding how the system will work, we need to understand the concept of cryptography, public-key encryption algorithms, and hashing.

Cryptography

Cryptography is a method of protecting information or establish secure communications through the use of codes called keys. The unique key is required to either encipher or decipher. Encipher is to encrypt plain text into ciphertext or encrypted text. Decipher is to decode that unintelligible message back into its original form using a key.

Types of Cryptographic System

1. Based on types of an operation used for encryption or decryption

    All encryption algorithms are usually based on two main principles: Substitution, in which elements are replaced with other characters from a table or something

else and Transposition, in which the positions of the characters are changed/rearranged.

2. The number of Keys used in the algorithm

   Symmetric key or single-key encryption, in which the sender and receiver both use the same key for encryption and decryption and Asymmetric or public-key encryption, in which the sender of the message and receiver of the message have different keys. The key used for encryption is different than the key required to decrypt the message. We will be using a very popular public-key encryption algorithm (RSA) in the cryptographic ID card and e-voting system.

3. The processing technique

   Block cipher, in which block of elements from the input is processed at a single time to produce an output block and Stream Cipher, in which each input element is converted to output element one after another.

All of these have their pros and cons. We will be using the RSA (Rivest-Shamir-Adleman) encryption algorithm which is a block-based, asymmetric cipher that uses both substitutions and transpositions for key generation and encryption.

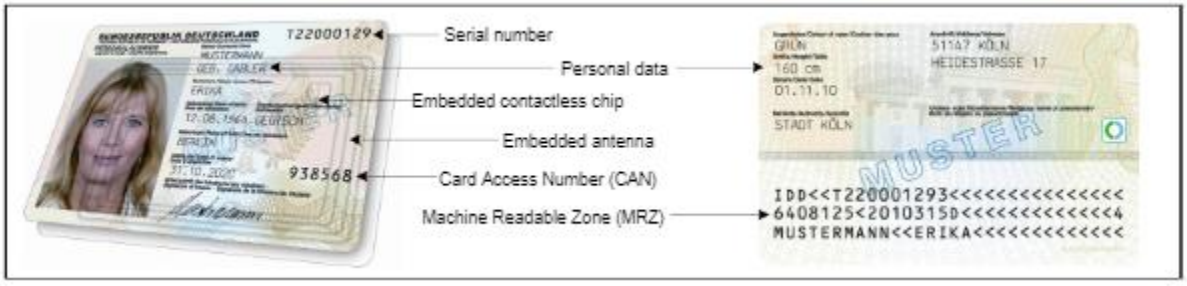

Figure 1 Front and Backside of the German E-ID Card

Electronic ID Cards for user identification / Authentication Scheme for Everyone

Many governments have public authentication systems that identify the citizens and store information about them which is beneficial for the government as well as the businesses where they need reliable information about persons and identify them. This new electronic ID card will provide a universal and secure authentication scheme for government and private sector applications with added privacy benefits. It will also help in systems using online authentication.

Applications for E-ID

There are many applications of such technology, it will help create a world where the id card replaces username and passwords, supports better identification and authentication of individuals, supports better business processes online and offline, and allow services to be provided online that require extensive paperwork in today's world. It could also be integrated with our bank accounts, a single card as your identity, bank credit card to check into hotels,

make reservations, file taxes, etc. This infrastructure will be so beneficial for not only the citizens but also the business owners and service providers.

- Government services that require the citizen's formal identification.
- Services that allows a citizen to view their personal data/information can identify the requester of the data easily.
- Banks and other businesses which need to store the personal information of their clients and want them to physically prove their identity can identify individual online.
- Operators of age-restricted services can confirm the age of the user easily.

These applications provide a view of how useful and beneficial, the adaptation of electronic ID cards can be.

These cards can also open the possibility of a very secure E-Voting System that we will discuss later and how Pakistan needs this type of system for its elections.

Electronic ID Functions

Digital Identities

Makes a subset of identity data accessible to an authorized requestor. Identity data stored in the card such as

- Names
- Date and place of birth
- Address

The biometric data will be stored in a government database in an encrypted format that can be decrypted using the private key associated with the public key stored in the card.

Cryptographic Protocols

Cryptographic protocols will be used to secure the communication between the card and the card reader. This system will work on the concept of digital signatures. A pin would be required to access the encrypted data as an added layer of security. This encrypted data can only be decrypted and verified using a private key from the government database that was used to create the public key stored in the card at the time of creation.

Security and Privacy Protocols

For the citizens, the use of cryptographic protocols ensures that their personal information is secure and that anyone can access the data

- Only with the consent of the card owner
- An authorize trusted service
- Within the limits allowed
- The data is protected from tampering and misuse

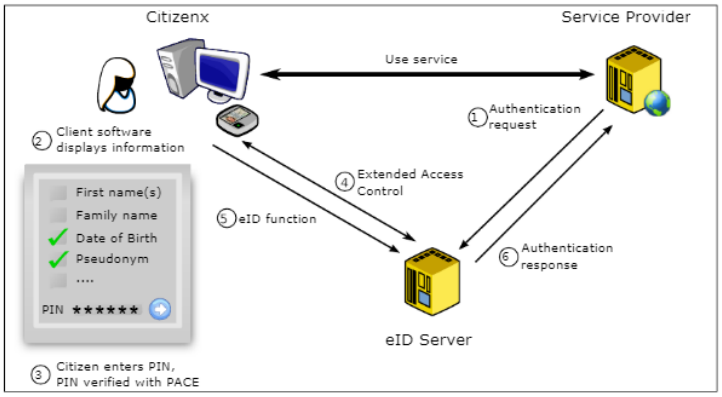

Figure 2 Online Authentication Process

The card chip authenticates the electronic ID server and verifies if it is authorized or not using certificates. If the card reader is equipped with a keypad, the PIN is used to protect against viruses and malicious software on the user's computer. Chip authentication also ensures that the data received by the service provider originated from a genuine, valid ID that was issued by the government using digital signatures.

Roles and Responsibilities

The implementation and operation of the electronic ID system are shared by the government and the private sector. The administrative agencies like NADRA register and issue ID Cards to the citizens. Federal administrative agencies decide which service providers should be authorized.

The private sector provides the servers and infrastructure to operate the E-ID system.

Citizens need a reliable card reader and client application.

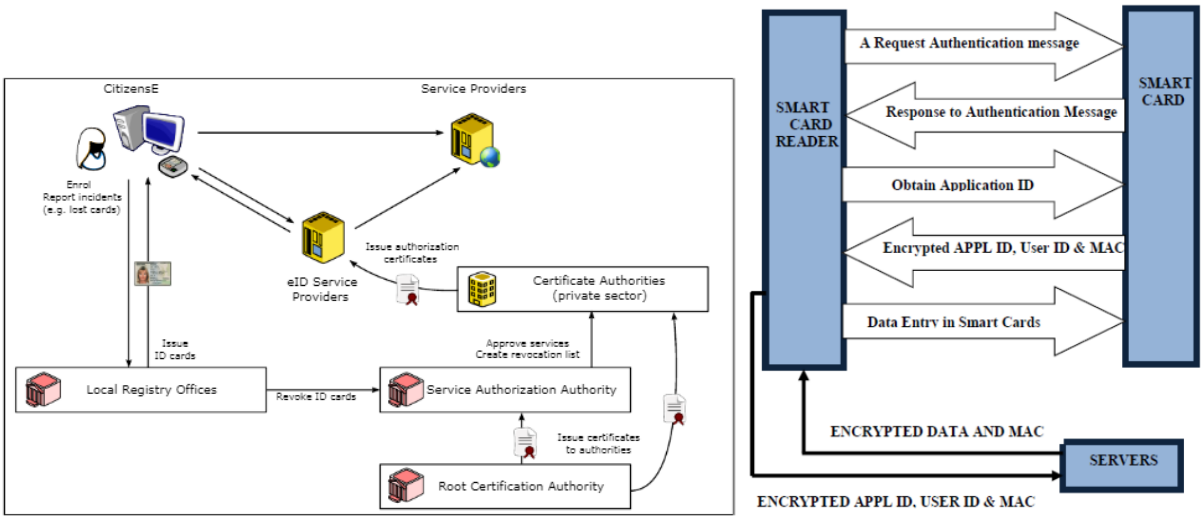

Figure 3 Left: Role and responsibilities for the new E-ID Card System Right: Authentication process in smart card

Design Rationale

The electronic ID systems design arises from a number of objectives and requirements.

User benefits

E-ID authentication is supposed to make the online authentication and identification much easier while allocating more control to the citizens

Service Provider Benefits

These ID cards provide reliable authentication procedures and maintain high-quality records. They can be used for general as well as legal authentication.

No Centralized Database

The public key algorithm and production of these cards are the only centralized components. Data required for card production can or will be deleted afterward.

Privacy Enhancements

The ID card will support on-card data verification.

E-Voting System

In Electronic ID systems, the private key is the ID. The private key is used by encrypting the checksum/hash value of the document that needs to be signed. This checksum proves the authenticity of the document and the integrity of the receiver. This is called a cryptographically signed document and the encrypted checksum is called a certificate. This is also the concept of digital signatures. This is the concept that is the basis for voting using an electronic voting system.

Elections and voting is an essential part of any democracy. With the recent advancements in Information Technology (IT), an Electronic voting system has appeared and is being continuously improved. Pakistan should adopt such a system as it brings many benefits that could improve the election procedure and smoothness. The E-Voting process involves:

- A computer as a voting terminal
- Voting web servers performing ballots processing and result counting in real-time
- The internet, to carry out the communication or data

The main benefits of E-Voting systems are

1. Cost-saving
2. Speed up the counting of the voting process
3. Increase citizens participation as the process is much simpler and secure
4. Allows citizens living abroad to easily participate in the elections as well

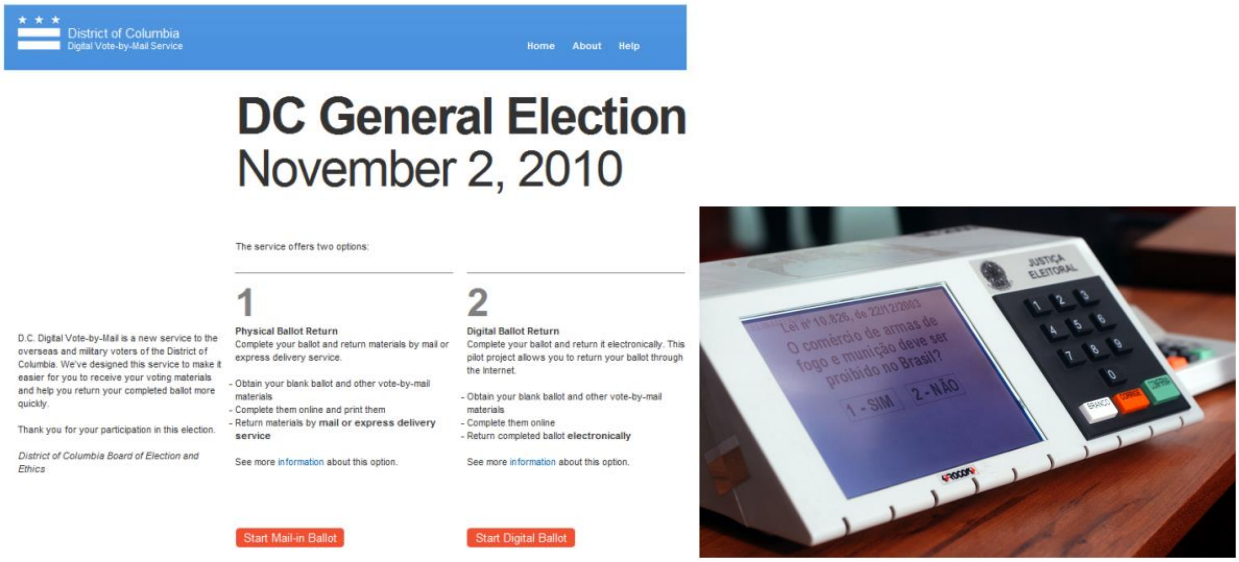

Figure 4 Left: Washington DC built an Internet voting system to allow overseas military voters Right: Brazil E-Voting Machine

Digital Signatures

Digital signatures are mathematical functions that help identify who sent a message or file. They provide much stronger proof of identification than the traditional signatures using a pen on a paper and are much more difficult to forge. In elections, the digital signatures are used to sign a vote, thus helping ensure that the vote or the system was not altered. For tempering, the attacker must know the secret key of once E-ID.

Hash Functions

Hashes are mathematical functions that simply read the binary or data of a file and produce a string or hash that is unique to that file. If anyone changes even a single character of the file, the hash value will completely change. SHA-256 is one of the popular hashing algorithms. Example the word “election” hashes to: c7a19845b9e9de079260094d79525957 using SHA-256. If we change it to “elections”, the hash will change to b9dd4e28c0fe5673909bb6c0615f5f22.

There are many applications of this concept in an E-Voting system. Using this we can detect if the vote cast is valid or not.

Conclusion

It is very unlikely that the Electronic ID Cards will soon replace other authentication mechanisms but it is becoming a viable solution as technology progresses and the encryption and secure communication techniques improve. E-ID Cards have huge potential and can become an enabler for new online applications. They provide the ease of authentication and

identification online that the traditional ID Cards provide offline. They can also be used to create a very secure and reliable E-Voting System.

Democracy relies on voters having well-founded trust in the process of voting i.e. vote's collection and count their votes. E-Voting systems can be considered as a milestone where citizens can voice their rights no matter where they live. E-Voting also improves voter turnout, as it is much more efficient, transparent and simpler. Pakistan can hugely benefit from adopting the E-ID and E-Voting system.

References

1. Cryptography (https://searchsecurity.techtarget.com/definition/cryptography)
2. RSA Algorithm (https://simple.wikipedia.org/wiki/RSA_algorithm)
3. Electronic Identity Cards for User Authentication – Promise and Practice (https://www.researchgate.net/publication/224260803_Electronic_Identity_Cards_for_User_Authentication-Promise_and_Practice)
4. Smart Card ID: An Evolving and Viable Technology (https://thesai.org/Downloads/Volume9No3/Paper_18-Smart_Card_ID_An_Evolving_and_Viable_Technology.pdf)
5. Estonian eID cryptography mess – 750000 cards compromised – Public Key Cryptography and E-Voting System (https://edri.org/estonian-eid-cryptography-mess-750000-cards-compromised/)
6. ID-based encryption (https://en.wikipedia.org/wiki/ID-based_encryption)
7. E-Voting evaluation report (https://www.researchgate.net/publication/296848330_E-Voting_evaluation_report)
8. The Important Uses of Cryptography in Electronic Voting and Counting (https://www.ndi.org/e-voting-guide/examples/cryptography-in-e-voting)
9. Electronic Voting (https://crypto.stanford.edu/pbc/notes/crypto/voting.html)
10. Electronic Voting Protocol Using Identity-Based Cryptography (https://www.hindawi.com/journals/tswj/2015/741031/)
11. Cryptographic Voting — A Gentle Introduction (https://eprint.iacr.org/2016/765.pdf)
12. Digital Signatures (https://en.wikipedia.org/wiki/Digital_signature)