CRYPTOGRAPHY ALGORITHMS for PERSONAL IDENTIFICATION VERIFICATION (PIV) SYSTEMS

Venu Shah[#1],Ashwin Iyengar[#2], Akshay Mahale[*3], Arjun Darak[#4], Vishal Kalal[#5]

Department of Electronics and Telecommunication, Atharva College of Engineering, University of Mumbai
First-Third Department, First-Third University
Address Including Country Name

[1]shah_venu@yahoo.com
[2]ashwin.iyengar92@gmail.com
[3]ArjunDarak@gmail.com
[4]amalale22@gmail.com
[5]vishalkalal1810@gmail.com

***Abstract*— Authentication of an individual's identity is a fundamental component of physical and logical access control processes. When an individual attempts to access security-sensitive buildings, computer systems, or data, an access control decision must be made. An accurate determination of an individual's identity is needed to make sound access control decisions. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to federally controlled government facilities and electronic access to government information systems. The control and security objectives include identity proofing, registration, and issuance. PIV Cards may support card activation by the card management system to support card personalization and post-issuance card update. PIV Cards that support card personalization and post-issuance perform a challenge response protocol using a symmetric cryptographic key (i.e., the PIV Card Management Key) to authenticate the card management system. After successful authentication, the card management system can modify information stored the PIV Card.**

Keywords— **Cryptography, public key, private key, digital Signatures and personal identification and verification Systems.**

I. INTRODUCTION

A wide range of mechanisms is employed to authenticate an identity, utilizing various classes of identity credentials. For physical access, an individual's identity has traditionally been authenticated [1] by use of paper or other non-automated, hand-carried credentials, such as driver's licenses and badges. Access authorization to computers and data has traditionally been based on identities authenticated through user-selected passwords. More recently, cryptographic mechanisms and biometric techniques have been used in physical and logical security applications, replacing or supplementing the traditional identity credentials.

The strength of the authentication that is achieved varies, depending upon the type of credential, the process used to issue the credential, and the authentication mechanism used to validate the credential.

This document describes standard for a Personal Identity Verification (PIV) [8] system based on secure and reliable forms of identity credentials issued by the Federal government to its employees and contractors. This Standard addresses requirements for initial identity proofing, infrastructures to support interoperability of identity credentials, and accreditation of organizations and processes issuing PIV [8] credentials.

II. NEED FOR SECURE AND RELIABLE FORM OF PERSONAL IDENTIFICATION

1. Based on sound criteria to verify an individual employee's identity.
2. Strongly resistant to fraud, tampering, counterfeiting, and terrorist exploitation.
3. Rapidly verified electronically.
4. Issued only by providers whose reliability has been established by an official accreditation process. [1][8]
5. Applicable to all government organizations and contractors except identification associated with National Security Systems.
6. Used for access to Federally-controlled facilities and logical access to Federally-controlled information systems.
7. Flexible in selecting appropriate security level – includes graduated criteria from least secure to most secure.

8. Implemented in a manner that protects citizens' privacy.

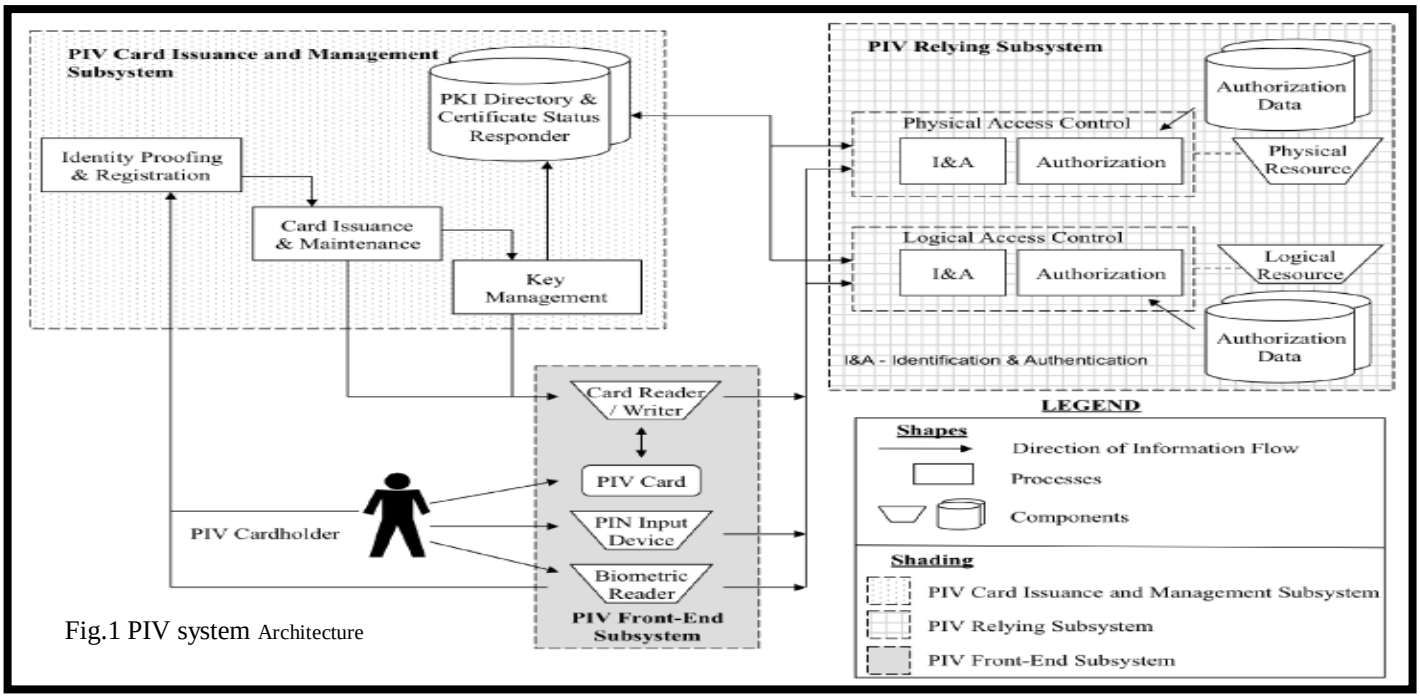

Fig.1 PIV system Architecture

III. PIV SYSTEM ARCHITECTURE[8]

The PIV system is composed of components and processes that support a common (smart card-based) platform for identity authentication across Federal departments and agencies for access to multiple types of physical and logical access environments. .

An operational PIV system can be logically divided into the following three major subsystems:

3.1 PIV Front-End Subsystem [8]—

PIV Card, card and biometric readers, and PIN input device. The PIV cardholder interacts with these components to ain physical or logical access to the desired Federal resource.

3.2 PIV Card Issuance and Management Subsystem[8]— the components responsible for identity proofing and registration, card and key issuance and management, and the various repositories and services (e.g., public key infrastructure (PKI) directory, certificate status servers) required as part of the verification infrastructure.

3.3 PIV Relying Subsystem[8]—
ntrol systems, the protected resources, and the authorization data. The PIV relying subsystem becomes relevant when the PIV Card is used to authenticate a cardholder who is seeking access to a physical or logical resource. The Standard does not provide technical specifications for this subsystem.[1] and authentication[1] are defined in Section 6 to provide

IV. CRYPTOGRAPHY ALGORITHMS FOR PIV SYSTEMS[2]

The PIV logical credentials shall contain multiple data elements for the purpose of verifying the cardholder's identity at graduated assurance levels.

The following mandatory data elements are part of the data model for PIV logical credentials that support authentication mechanisms interoperable across agencies:

- a PIN
- a CHUID
- PIV authentication data (one asymmetric key pair and corresponding certificate)
- two fingerprint templates
- an electronic facial image
- card authentication data (one asymmetric key pair and corresponding certificate).

The Standard also defines two data elements for the PIV data model that are mandatory if the cardholder and are: an asymmetric key pair and corresponding certificate for digital signatures; and an asymmetric key pair and corresponding certificate for key management.
The Standard also defines optional data elements for the PIV data model. These optional data elements include: one or two iris images; one or two fingerprint templates for on-card comparison;a symmetric Card Authentication key for supporting physical access applications; and a symmetric

PIV Card Application Administration key associated with the card management system.
The logical credentials fall into the following three categories:

1. credential elements used to prove the identity of the cardholder to the card (CTC authentication);

2. credential elements used to prove the identity of the card management system to the card (CMTC authentication); and

3. credential elements used by the card to prove the identity of the cardholder to an external entity (CTE authentication) such as a host computer system.

4.1 PIN
The PIN falls into the first category, the PIV Card Application Administration Key into the second category, and the CHUID, biometric credentials, symmetric keys, and asymmetric keys

into the third. The fingerprint templates for on-card comparison fall into the first and third categories.

4.2 Cardholder Unique Identifier (CHUID)
The CHUID includes the Federal Agency Smart Credential Number[4] (FASC-N) and the Global Unique Identification Number[4] (GUID), which uniquely identify each card. The value of the GUID data element shall be a 16-byte binary representation of a valid Universally Unique IDentifier (UUID). The CHUID shall also include an expiration date data element in machine-readable format that specifies when the card expires.

The asymmetric signature data element of the CHUID shall be encoded as a Cryptographic Message Syntax (CMS) external digital signature. Algorithm and key size requirements for the asymmetric signature and digest algorithm.

4.3 PIV authentication data:

Public-key algorithms are asymmetric algorithms and, therefore, are based on the use of two different keys, instead of just one.

In public-key cryptography, the two keys are called the private key and the public key.

Private key must be known only by its owner while Public key is known to everyone (it is public).

Public key required to verify the digital signature shall be provided in the certificates field of the CMS external digital signature in a content signing certificate.

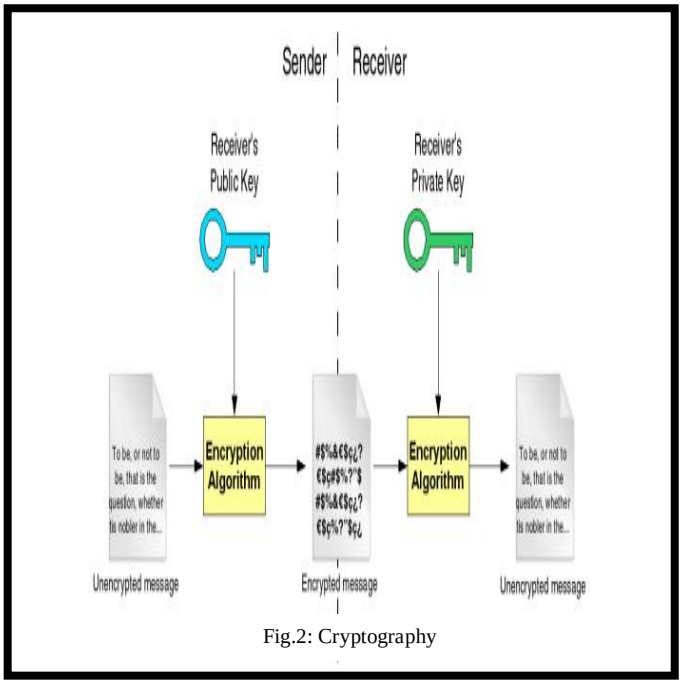

Fig.2: Cryptography

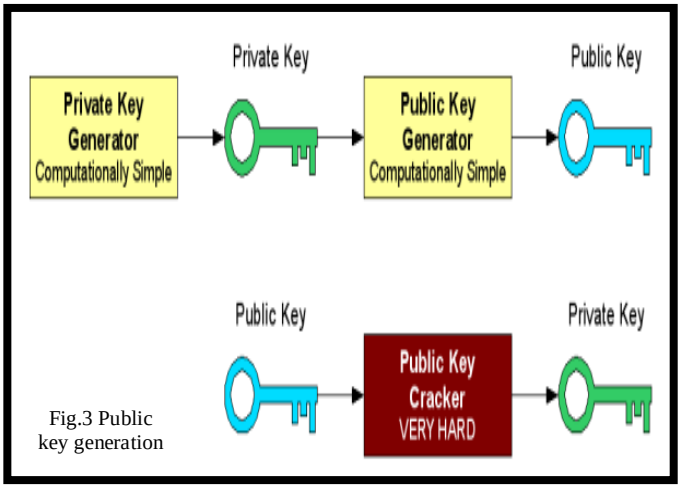

Fig.3 Public key generation

The digital signature for a message is generated in two steps:

A *message digest* is generated. A message digest is a 'summary' of the message we are going to transmit, and has two important properties: It is always smaller than the message itself and even the slightest change in the message produces a different digest. The message digest is generated using a set of hashing algorithms. The message digest is encrypted using the sender's *private* key. The resulting encrypted message digest is the *digital signature*.

minimum, the PIV Card must store two asymmetric private keys and the corresponding public key certificates, namely

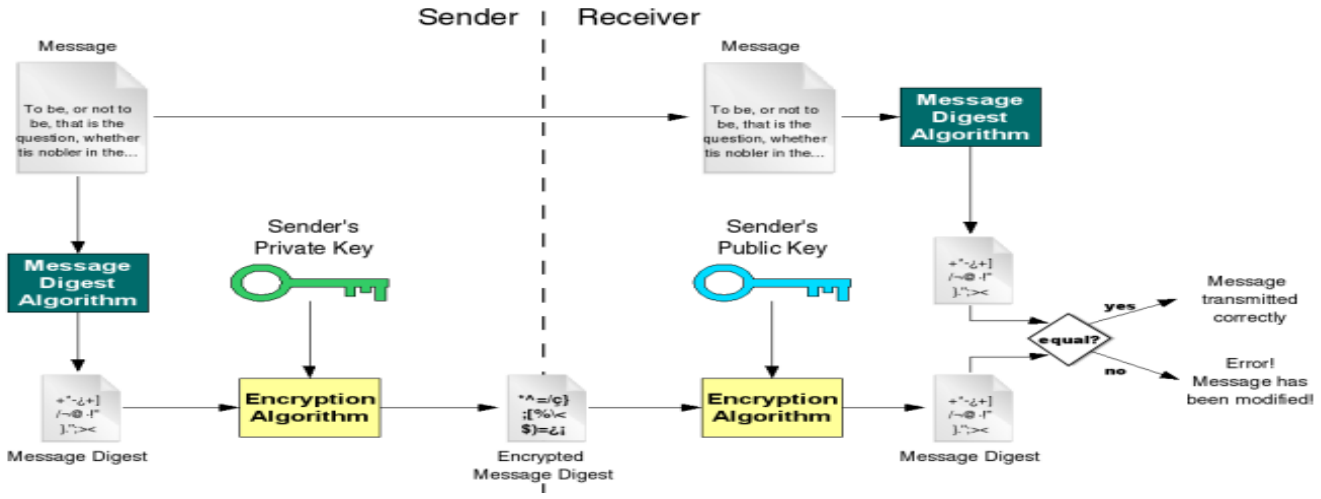

Fig. 4: Digital Signature

The digital signature is attached to the message, and sent to the receiver. The receiver then does the following:

Using the sender's public key, decrypts the digital signature to obtain the message digest generated by the sender.

Uses the same message digest algorithm used by the sender to generate a message digest of the received message.

Compares both message digests (the one sent by the sender as a digital signature, and the one generated by the receiver). If they are not *exactly the same*, the message has been tampered with by a third party. We can be sure that the digital signature was sent by the sender (and not by a malicious user) because *only* the sender's public key can decrypt the digital signature (which was encrypted by the sender's private key; remember that what one key encrypts, the other one decrypts, and vice versa). If decrypting using the public key renders a faulty message digest, this means that either the message or the message digest are not exactly what the sender sent.

4.4 Biometric data

It includes:

1) One or two iris images.
2) Fingerprint templates for on-card comparison.

IV. CRYPTOGRAPHY SPECIFICATIONS FOR PIV SYSTEMS

The PIV Card must store private keys and corresponding public key certificates, and perform cryptographic operations using the asymmetric private keys. At a minimum, the PIV Card must store two asymmetric private keys and the corresponding public key certificates, namely the PIV Authentication key and the asymmetric Card Authentication key. The PIV Card must also store a digital signature key and a key management key, and the corresponding public key certificates, unless the cardholder does not have a government-issued email account at the time of credential issuance.

A. The PIV Authentication key is a mandatory asymmetric private key that supports card and cardholder authentication for an interoperable environment.
B. The asymmetric Card Authentication key is a mandatory private key that supports card authentication for an interoperable environment.
C. The symmetric (secret) Card Authentication key supports card authentication for physical access, and it is optional.
D. The digital signature key is an asymmetric private key supporting document signing.
E. The key management key is an asymmetric private key supporting key establishment and transport. Optionally, up to twenty retired key management keys may also be stored on the PIV Card.
F. The PIV Card Application Administration Key is a symmetric key used for personalization and post-1320 issuance activities, and it is optional.

Conclusion

The PIV system has to be extremely secured and the cryptography algorithms [2],[3],[4],[5], [6] and keys are very important in deciding the complete integrity and confidentiality of the data. PIV card data has to be handled properly and other than cryptography iris or face or any other biometric based accession must be used.

Acknowledgment

We are immensely thankful for the active cooperation of all faculties of Electronics and Telecommunications department and IEEE student council of AET's Atharva College of Engineering. Their advice and support has been very helpful in making this effort of writing the paper possible.

REFERENCES

[1] M.Bellare and P.Rogaway.Entity Authentication and key distribution Advances in Cryptology - Crypto 93 Proceedings, Lecture Notes in Computer Science Vol. 773, D. Stinson ed, Springer-Verlag, 1994.

[2] Advance cryptography algorithm for improving data security by Vishwa gupta, Gajendra Singh and Ravindra Gupta published in International Journal of Advanced Research in Computer Science and Software Engineering on Volume 2, Issue 1, January 2012.

[3] Data Hiding and Retrieval, A.Nath, S.Das, A.Chakrabarti, Proceedings of IEEE International conference on Computer Intelligence and Computer Network held at Bhopal from 26-28 Nov, 2010.

[4] Neal Koblitz "A Course in Number Theory and Cryptography" Second Edition Published by Springer-Verlag.

[5] Majdi Al-qdah & Lin Yi Hui "Simple Encryption/Decryption Application" published in International Journal of Computer Science and Security, Volume (1) : Issue (1).

[6] T Morkel, JHP Eloff "ENCRYPTION TECHNIQUES: A TIMELINE APPROACH" published in Information and Computer Security Architecture (ICSA) Research Group proceeding.

[7] Text book by William Stallings, "Data and Computer Communications" , 6e William 6e 2005.

[8] http://www.ftc.gov/os/2008/02/hrpd12pia.pdf