***Protocol and Standards:***

1. **NFC:** NFC or Near Field Communication is a wireless communication technology that enables the transfer of data using a proximity of up to 10 cm. It is a very simple technology where transactions are initialized automatically by touching a reader or NFC device [1]. This is bidirectional coupling technology which is based on standard ISO 14443. The standard ISO 18092 is responsible for the peer-to-peer mode of the physical and data-link layer of NFC.
2. **ISO/IEC 14443 Protocol:** With RFID systems, there are numerous standards still being used. The ISO/IEC 14443 [2] specification is one of the most widely used standards for proximity cards, which have a transmission range of roughly 15 cm. A tag is referred to in 14443 as a PICC (proximity integrated circuit card), while a device is referred to as a PCD (proximity coupling device). Under the ISO/IEC 14443 standard, there are two types: Type A and Type B, both of which communicate by radio at a frequency of 13.56 MHz (RFID HIGH FREQUENCY). The primary distinctions between these two types relate to protocol initiation procedures, coding schemes, and modulation schemes. The transmission methodology is the same for both types of RFID cards. Since the protocol stack is entirely transparent, the ISO/IEC 14443 standard does not provide any security procedures. The ISO/IEC 14443 standard defines a Waiting Time Ex- tension (WTX) command. This command can be used by a PICC to request more time to prepare the response. In view of relay attacks, the command can be exploited to obtain more time to relay the data.
3. **ISO 18092:** It standardizes peer-to-peer communication mode for random binary data exchanges. The peer-to-peer mode has a very big role in creating a secondary high-speed connection like Bluetooth or WiFi for the transfer of a large amount of data using NFC [3]. Devices can read or write data of any supported tag types in a standard data format because of this standard. Exchange of data over custom binary protocol is also enabled between devices. Card emulation allows the phone to act as a tag (contactless card) for other readers or POS terminals.
4. **Secure Electronic Transaction (SET) Protocol:** In the world of electronic commerce, SET Secure Electronic Transaction is regarded as the key contributor to the payment system. It is an extremely thorough security mechanism that makes use of cryptography to ensure data secrecy. It guarantees both identity identification and payment integrity. The SET protocol's primary and fundamental requirement is that electronic transactions be carried out securely. SET employs two primary types of cryptography—public-key cryptography and secret-key cryptography—as well as techniques for encryption and decoding. A business can generate a public or private key pair and broadcast the public key using public key cryptography. This enables any client to send a secure message to the business. Financial institutions adopt DES (Data Encryption Standard), secret key cryptography, instead of RSA, public key cryptography, to encode PIN numbers [4].
5. **ISO/IEC 7816 Protocol:** The characteristics of a card that has been bent or flexed are described by ISO7816-1 [5]. This is done to ensure that plastic cards with embedded chips are made in a way that ensures immaculate performance over the duration of a card's estimated life. The connections between the surface connectors and the embedded silicon die's I/O pins must resist mechanical stress and stagnate. Procedures for bending and flexing are standardized in ISO 7816. Although vendor-specific application layer protocols are occasionally used, the ISO/IEC 7816-4 application protocol is most frequently chosen. For card producers, this portion of ISO7816 is crucial. They select the components and set up the procedure for integrating the integrated circuit into the card. Some such smart cards produced before 1990 adhered to a different standard for the contact location and cannot be utilised with modern smart card readers that are ISO 7816-2 compliant. The majority of these cards were used in Europe. It should be noted that there is no space for embossing in the thickness dimension. More specifically, the card slot may have an additional notch for the embossed portion of the card. In effect, it functions as a polarization key and can be used to help the card be inserted correctly. The magnetic field sensor, which relies on the magnetic stripe and opens a mechanical gate on devices like ATMs where some vandal-proofing measures are applied, has this extra feature.
6. **ISO 8583:** A standard for systems that exchange electronic transactions using payment cards. It defines the message format and the communication flow to enable the exchange of transaction requests and responses between different systems [6]. As per reports, most commonly Mastercard, Visa and Verve networks base their authorization communications in this standard. This standard is not directly used by systems or networks. This standard defines many data fields which are retained in the same systems and later used by each network to adapt the standard with custom usage. The main objective of this ISO protocol is to transfer information for payments via a network using TCP/IP sockets.
7. **ISO 7810:** This standard defines the physical characteristics of identification cards. It specifies physical dimensions, resistance to bending, chemicals, temperature, humidity, and toxicity. There are four card sizes and that are ID-1 which is mostly banking and ID cards, ID-2 which is for Romanian and other ID cards and visas as well, ID-3 this size is for passport booklets and fourth ID-000 is for sim cards. The standard also defines the metric and imperial measurements for the card[7][8].
8. ***NFCIP-1and NFCIP-2*: *Near Field Communication Interface and Protocol***

At information transmission speeds of 106, 212, and 424 kbps, this protocol is described in standards ISO/IEC 18092 and ECMA-340. It specifies modulation, coding, and frame structure [9]. An initiator and a target form the object of communication in NFC. The main methods offered by NFCIP-1 are RFCA (Radio Field Collision Avoidance) and SDD (Single Device Detection) [10]. The SDD is an algorithm that helps the initiator select a particular target from a group of targets in the RF field. Collision issues might arise with the current RFID technology. A scenario when more than two initiators or targets communicate data simultaneously and it is difficult to tell whether data is real is referred to as a collision. The NFC standard uses the RFCA algorithm to tackle the collision problem. RFCA is a method that uses carrier frequency to find additional RF fields and avoid collisions. The first step of RFCA is to validate the existence of other RF fields. The NFC does not produce its own RF field if other RF fields are already present. The SDD, which locates particular targets within the range, and the RFCA, which forbids the use of two RF fields, allow the NFC to be protected from the attacks like MITM (Man-In-The-Middle).

The NFCIP 2 protocol operates at the ECMA 352 standard and specifies how to select a communication method between the three states described in ECMA 340 to ISO/IECS 14443 and ISO/IEC15693 [9].

1. **ECMA 385 & ECMA 386:**

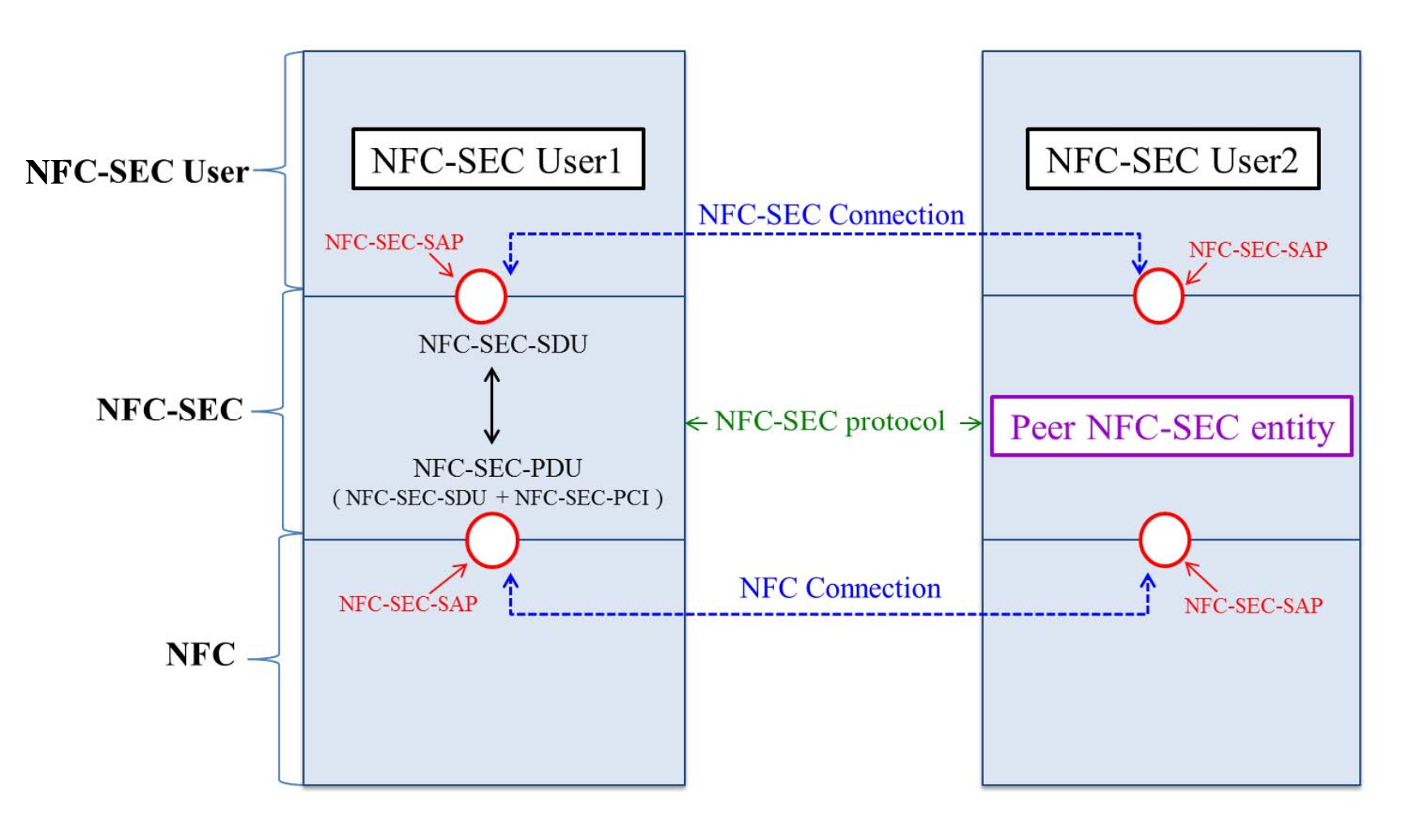
****

Fig 1. ECMA 385 standard structural model

The Secure Channel Service (SCH) and the Shared Secret Service (SSE) are two services that are supported by ECMA 385 and ECMA 386 [11]. The Open System Interconnection Reference Model (OSI Reference Model) served as a design guide for ECMA 385's organizational structure. The ECMA 385 standard structural model is shown in Fig 1[12]. It separated NFC-SEC User, NFC-SEC, and NFC into three levels. The NFC-SEC standard prevents data modulation and eavesdropping by unidentified third parties. Now, if an NFC user1's phone wishes to contact another NFC user, it must engage the NFC-SEC-SAP (Service Accessing Point) request service. The request from the user will be noted in the NFC-SEC-SDU (Service Data Unit). The NFC-SEC-PDU (Protocol Data Unit) is created by combining the NFC-SEC-SDU and the NFC-SEC-PCI (Protocol Control Information). With User1's NFC-SEC- SAP, which sits at the intersection of the NFC-SEC layer and the NFC layer, the NFC-SEC- PDU may establish a "NFC connection" with the NFC-SEC User2's NFC-SEC-SAP. They will be motivated to coordinate a common secret value for further communication by this conduct. It is known as the Secure CHannel service (SCH) in the ECMA 386 standard. In the ECMA 386 standard, the Shared SEcret service (SSE) was defined. To create their secret keys, they will employ the Diffie-Hellman Elliptic Curve technique. They would begin to transmit after creating the SCH and SSE during the connecting phase.

The ECMA 385 standard and the ECMA 386 standard both specify these two services. Nevertheless, the Card Emulated Mode and Reader/Writer Mode do not support these two secure transaction protocols. Only the peer-to-peer mode may be employed with these two services.

***References***

1. Madlmayr, Gerald, Josef Langer, Christian Kantner, and Josef Scharinger. "NFC devices: Security and privacy." In *2008 Third International Conference on Availability, Reliability and Security*, pp. 642-647. IEEE, 2008.
2. Issovits, Wolfgang, and Michael Hutter. "Weaknesses of the ISO/IEC 14443 protocol regarding relay attacks." In *2011 IEEE International Conference on RFID-Technologies and Applications*, pp. 335-342. IEEE, 2011.
3. <https://bitexperts.com/Question/Detail/3360/difference-between-iso-14443-and-iso-18092-i-e-rfid-vs-nfc>
4. Parihar, Pankaj Singh, Vikas Kurdia Pankaj Suwalka, and Ratnesh Parasher Deepali Mahatma. "An Implementation of Set Protocol with DES Algorithm."
5. Thorpe, Christina, John Tobin, and Liam Murphy. "An ISO/IEC 7816-4 Application Layer Approach to Mitigate Relay Attacks on Near Field Communication." *IEEE Access* 8 (2020): 190108-190117.
6. <https://en.wikipedia.org/wiki/ISO_8583>,<https://www.ir.com/guides/introduction-to-iso-8583>
7. [Early Discovery of Chronic Non-attenders by Using NFC Attendance Management System](https://ieeexplore-ieee-org.lib-ezproxy.concordia.ca/document/6624813), <https://en.wikipedia.org/wiki/ISO/IEC_7810>
8. Ochomo, Zablon O., Elisha Opiyo, William Okello-Odongo, and J. M. Kizza. "Agent Based Model For Localized Secure Payment Systems Integration." *Strengthening the Role of ICT in Development* (2010).
9. Shariati, S. Mahdi, A. Abouzarjomehri, and M. Hossein Ahmadzadegan. "Investigating NFC technology from the perspective of security, analysis of attacks and existing risk." In 2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI), pp. 1083-1087. IEEE, 2015.
10. Eun, Hasoo, Hoonjung Lee, and Heekuck Oh. "Conditional privacy preserving security protocol for NFC applications." IEEE Transactions on Consumer Electronics 59, no. 1 (2013): 153-160.
11. Chen, Cheng Hao, Iuon Chang Lin, and Chou Chen Yang. "NFC attacks analysis and survey." In 2014 eighth international conference on innovative mobile and internet services in ubiquitous computing, pp. 458-462. IEEE, 2014.