TELKOMNIKA, Vol.17, No.2, April 2019, pp.712~718
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v17i2.11755

KAFA: A novel interoperability open framework to utilize Indonesian electronic identity card

Rolly Maulana Awangga*, Nisa Hanum Harani, Muhammad Yusril Helmi Setyawan
Applied of Informatics Engineering Politeknik Pos Indonesia, Indonesia
*Corresponding author, e-mail: awangga@poltekpos.ac.id

Abstract

Indonesian people have electronic citizen card called e-KTP. e-KTP is NFC based technology embedded inside Indonesian citizenship identity card. e-KTP technology has never been used until now since it was launch officially by the government. This research proposes an independent framework for bridging the gap between Indonesia regulation for e-KTP and commercial use in the many commercial or organization sector. The Framework proposes interoperability framework using novel combination component, there are e-KTP reader, Middleware and Web Service. KAFA (e-KTP Middleware and Framework) implementing Internet of Things (IoT) concept to make it as open standard and independent. The framework use federation mode or decentralized data for interoperability, to make sure not breaking the law of privacy. Extended development of AES-CBC cipher algorithm was used to encrypt the data on the transport between middleware and web service.

Keywords*: AES-CBC, e-KTP, interoperability, KAFA, web service*

1. Introduction

The use of ID on identity is essential as a single identity number that distinguishes one data from another. As stated in the Presidential Regulation of The Republic of Indonesia Number 35 The Year 2010 that NIK-based ID cards contain security codes and electronic recordings as a means of verifying and validating the identity data of the population [1]. Currently, Indonesia applies the identity identifier with a technology-based identity card system with electronic ID card (e-KTP card). The e-KTP card technology is the technology incorporated into the contactless smart card technology [2]. The identity or resident information of the e-KTP card stored in a data center [3] and stored in a physical form of an e-ID card. e-KTP use Near Field Communication (NFC) technology. NFC is a short-range radio technology that allows communication between devices by touching each other or holding adjacent devices [4]. NFC itself is quite simple, done by using radio frequency. NFC device itself is divided into two classes, namely the target device and initiator [5]. Near Field Communication (NFC) is one of the new technologies used in faster, cheaper and more secure data transfers [4].

At the present time, several research in e-KTP card among others can be used for the needs in transactional activities that assist in the validity of the data for example in the general election system [6] besides e-KTP card can be used as a tool in home security system [7]. and has been im-plemented in several sectors, including electronic payments [4]. In this case, there is a gap problem in interoperability standard for using e-KTP to integrate in the organization process business. In the logistics sector for example, require consumer data such as data sender and receiver. Currently, there are many disadvantages in logistic distribution schemes, such as consumer information errors. Also, the use of paper in recording consumer information is quite tricky because the courier must perform manual authentication data [8]. So with the e-KTP card can be used for authentication of data validity so that data used more accurate compared to manual recording. Frameworks are used as guides to build something that extends the structure into something useful. TOGAF is a framework that provides detailed methods for building and managing enterprise information sys-tems and architectures [9]. TOGAF can optimize the overall aspect of the company's environment in order to respond to changes. This framework is suitable for designing corporate governance. Federation Model is a method in enterprise architecture that allows interoperability and division of business lines and information technology semi-autonomously. This research proposes a novel interoperability Framework for

Received August 6, 2018; Revised October 20, 2018; Accepted December 25, 2018

e-KTP. The framework proposing as open standard and independent using open hardware and software.

2. Research Method

KAFA (e-KTP Middleware and Framework) is a framework developing using IoT concept. IoT is a concept that has the purpose of expanding the benefits of internet connection. In IoT it provides connectivity on physical sensors that can generate messages between objects. IOT works by translating the programming language we have put into the tool called Microcontroller. Arduino provides you with a library that is relatively clean, and trades flexibility for simplicity. Given the data, the AES-CBC method involves a process of encryption and decryption that can produce plaintext. AES-CBC cipher algoritm was use to secure communication flow. And to be able to visualize all the models in one tool we will use the concept of federation modeling.

2.1. IoT

The IoT concept is that we can connect, communicate and manage multiple devices au-tomatically with countless remote networks. It is a scenario in which storage, computing and communication technologies are embedded in everyday objects. Processing, storage and commu-nication capabilities attached to an object turns object into a service for which users pay per use [10]. Web service is also a big part of IoT. The low computational web service [11] also developing in this research.

2.2. Open Hardware

Arduino is an open-source platform to facilitate the use of electronics in various fields. Arduino uses Atmel AVR processor and its software has its own programming language (often referred to as a microcontroller) or IDE (Integrated Development Environment) that runs on your computer, used to write and upload computer code to the physical board. IDE is a software used to write and compile programs for Arduino. Arduino IDE is also used to upload compiled programs to the Arduino board program memory [7].

2.3. NFC

Near Field Communication (NFC) is a kind of communicational technology, which run wirelessly at a high frequency; and it can work in 20 cm by 13.56 MHz. It can transmit data at three speeds which are respectively 106 Kbit/s, 212 Kbit/s and 424Kbit/s. The NFC has two work modes which are initiative mode and passive mode [12]. Card emulation mode: In this mode, the NFC tag is equivalent to an IC card which adopts RFID technology. The NFC tag can replace many IC cards used now (including credit, card entrance card used in supermarket, easy card, control card, ticket to vehicle, ticket to door and so on). In this mode, it is a great advantageous that the RF domain of Non-contact card reader can supply power to NFC tags; so, the tag can work even the host device is out of battery. The NFC tag must be equipped with Security Element (SE for short) if it wants to apply the function of Card Emulation [8].

NFC reader has two tasks, receive commands from software and communicate between NFC tags. NFC reader is a link between software applications with antenna will radiate radio waves to NFC tags. Radio waves emitted by the antenna gathered in the room around it. so that the data can be transferred wirelessly from or to the NFC tag located adjacent to the antenna [13]. In this discussion, NFC reader built by two microcontrollers that are arduino UNO board and NFC shield PN532. Communications between arduino UNO board and NFC shield PN532 can be using I2C (Inter-Integrated Circuit Communications, pronounced I squared C) protocol or SPI (Serial-Peripheral or Interface) protocol [14].

2.4. AES-CBC URL Encrypt

AES-CBC is one of the standard methods of encryption also known as The Rijndael algorithm [15]. AES is a symmetric key algorithm to helps prevent information from being passed in clear text. Both the sender and the receiver use a single key for encryption and decryption of up to 16 characters, and an initialization vector. [16]. This process requires a minimum of 128 bits of data in the encryption. The AESCBC method involves an Initialization Vector (IV) for XOR operations. Both encryption and decryption process is done with a key.

They must have a data length of 128 bits [17]. The process of encryption and decryption is as follows: To perform an encryption operation, a plaintext must have a length of multiple data of 128 bits XOR and IV will be operated on the first plaintext before it is encrypted by the key. The encryption process creates a ciphertext. Then it will be decrypted by the key first. After the decryption process, XOR operation and IV are performed to the decryption result to produce plaintext [16].

AES-CBC is adopted by many organizations around the world. Because it has simplicity and flexibility in the implementation stage. AES-CBC is used in various applications ranging from smart cards to large servers. In fact, hardware implementations of AES are well suited to resource-constrained embedded applications like satellites [16]. Several other advantages of choosing AES-CBC is that these are symmetric key ciphers, lightweight and more secured when compared to others [18]. The cipher is merged with the created instance of the AES algorithm [19]. Typically, the CPU memory on these IoT devices is a scarce resource. Hence, implementation of AES CBC will not cause memory footprint overloads [18].

2.5. Federation Model

The federation model best suits in the situation where an existing collection of autonomous and possibly heterogeneous databases are required to be shared. After authentication, the user can request data from any one of the databases within the federation. The owner institution has full control over local databases and has liberty of choosing among different configurations for different levels of autonomy, degree of replication, and cross-registration of each data resource [20]. The Cloud Architecture also implementing Federation model as single-sign-on authentication [21], real-time application [22], a service model [23], scalable peer-to-peer approach [24], and a reservoir model [25].

3. Experiment and Results

KAFA consisting three parts of platform shows in Figure 1 the reader, IoT and database. e-KTP Reader is an open hardware now with arduino and PN532 sensor. Middle-ware has bridging between e-KTP Reader to Web Service. Middleware read serial communication from e-KTP Reader using USB and pass it to the Web Service.

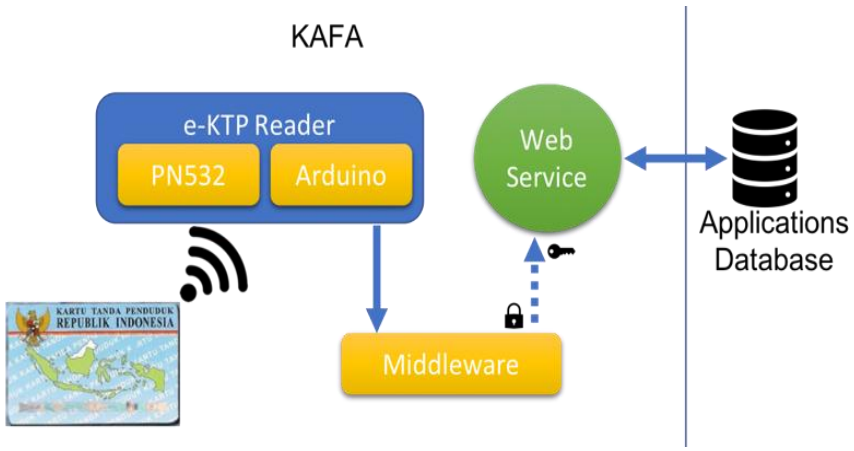

Figure 1. Architecture design of KAFA

URL Encryption was used between Middleware and Web Service using AES-CBC cipher algoritm base additional random character called Cilok Library. The algorithm of Cilok library shows in Figure 2, Cilok is a library that uses AES CBC. Web Service receive e-KTP ID data from Middleware and follow up to the next process in Application or Database. Application and Database is business process area where is it come from any service of Application to integrate with e-KTP Open Middleware Platform.

```python
def rndm(ln):
    ALPHABET = "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ"
    chars=[]
    for i in range(ln):
        chars.append(random.choice(ALPHABET))
    return "".join(chars)

def urlEncode16(uri):
    ln = len(uri)
    multihex = (ln/16)*16+16
    sp = multihex - ln - len(str(ln))
    if ln>9:
        dt = str(ln)+uri+rndm(sp)
    else:
        dt = "0"+str(ln)+uri+rndm(sp-1)
    return encodeData16(dt)

def urlDecode16(uri):
    if len(uri)%16 == 0:
        dt = decodeData16(uri)
        try:
            int(dt[:2])
            ln = int(dt[:2])
            ret = dt[2:2+ln]
        except ValueError:
            ret = dt
    else:
        ret = uri
    return ret
```

Figure 2. AES-CBC function on python code

3.1. e-KTP Reader

Open Hardware was chosen to built e-KTP Reader to fullfill Open Standar of this Frame-work. e-KTP reader consisting PN532 sensor and Arduino. PN532 Sensor connects ed to Arduino to read NFC on e-KTP. The wiring between arduino and PN532 sensor shows in Table 1. PN532 has set in the I2C mode. After wiring, the code from 3 push to the Arduino, Figure 3 show some code in Arduino to read NFC tags in e-ktp. The readers read NFC ID of e-KTP and pass it to serial communication to the computer.

untitled 2

```
#include <Wire.h>
#include <Adafruit_NFCShield_I2C.h>
#define IRQ   (2)
#define RESET (3)
Adafruit_NFCShield_I2C nfc(IRQ, RESET);
void setup(void) {
  Serial.begin(115200);
  Serial.println(">http://www.github.com/awangga/NFCReader");
  nfc.begin();
  uint32_t versiondata = nfc.getFirmwareVersion();
  if (! versiondata) {
    Serial.print(">Didn't find PN53x board, please close and open serial monitor. If problem still exist please check your wiring");
    while (1); // halt
  }
  Serial.print(">Found chip PN5"); Serial.println((versiondata>>24) & 0xFF, HEX);
  Serial.print(">Firmware ver. "); Serial.print((versiondata>>16) & 0xFF, DEC);
  Serial.print('.'); Serial.println((versiondata>>8) & 0xFF, DEC);
  nfc.SAMConfig();
}
void loop(void) {
  boolean success;
  uint8_t uid[] = { 0, 0, 0, 0, 0, 0, 0 };  // Buffer to store the returned UID
  uint8_t uidLength;                        // Length of the UID (4 or 7 bytes depending on ISO14443A card type)
  success = nfc.readPassiveTargetID(PN532_MIFARE_ISO14443A, uid, &uidLength);
  if (success) {
    nfc.PrintHex(uid, uidLength);
    uint8_t keya[6] = { 0xD3, 0xF7, 0xD3, 0xF7, 0xD3, 0xF7 };
    success = nfc.mifareclassic_AuthenticateBlock(uid, uidLength, 4, 0, keya);
    uint8_t data[16];
    success = nfc.mifareclassic_ReadDataBlock(4, data);
    nfc.PrintHexChar(data, 16);
    delay(1000);
  }
}
```

Figure 3. Arduino code to read e-KTP ID

Table 1. PN532 and Arduino Wiring

PN532 Sensor Pin	Arduino Pin
VCC	5V
GND	GND
SDA	A4
SCL	A5

3.2. Middleware and Web Service Deployment

The middleware code using python shows in Figure 4. The e-KTP ID passes from Mid-dleware to web service after encrypted using AES-CBC cipher algorithm in Figure 4. The Web service receiving e-KTP ID data and decrypt is. The web service code shows in Figure 5. The web service is customable to connect many API or Application or database in existing business environment. The demonstration shows in Figure 6.

```
main.
1  import serial
2  import webbrowser
3  from lib.cilok import urlEncode16
4  from lib import config
5
6
7  ser = serial.Serial(config.port, config.baudrate)
8  temp = ''
9  while 1:
10     data=ser.readline().rstrip('\n')
11     #print data
12     data=data.strip()
13     print data
14     if data[:1]=="[":
15         print "\a"
16         trimdata = data.replace(" ","")
17         thedata = urlEncode16(trimdata)
18         uri = config.keyuri+'%input%ktp%'+trimdata
19         thedata = urlEncode16(uri)
20         webbrowser.open_new(config.host+thedata)
```

Figure 4. ser2http middleware to establish communication between arduino and web service

```
main.py
1  import serial
2  from lib import cilok,config
3  from flask import Flask,abort
4  app = Flask(__name__)
5
6  @app.route("/<gurih>")
7  def get(gurih):
8      if gurih != cilok.urlDecode16(gurih):
9          return "e-KTP ID is : %s" % cilok.urlDecode16(gurih)
10     else:
11         abort(401)
```

Figure 5. e-KTP 1.0 web service code using python flask

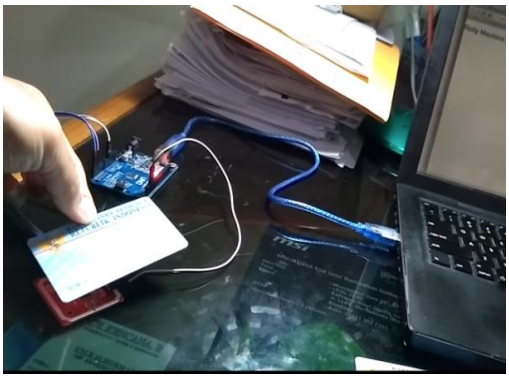

Figure 6. e-KTP device demonstration

4. Conclusion

KAFA is a first release of open standard for e-KTP interoperability. The framework is independent for utilizing indonesian electronic identity card into many business process.

The connection of Interoperability can develop in many ways using web service on Framework. Every components in Framework can be develop to the next version of Framework. e-KTP reader can be replaced with other sensor or device which is open hardware. Middleware development can be use another programming and implement more efficient encryption to be more functional. Communication between Middleware and Web Service can be develop in others internet protocol.

Acknowledgement

This research was funded by Direktorat Riset dan Pengabdian Masyarakat, Direktorat Jendral Penguat Riset dan Pengembangan Kementrian Riset, Teknologi, dan Pendidikan Tinggi Republik Indonesia by Penelitian Dosen Pemula Scheme.

References

[1] Sekretariat Negara. Presidential Regulation of The Republic Of Indonesia Number 35 OF 2010 (in Indonesia: Peraturan Presiden Republik Indonesia Nomor 35 Tahun 2010). 2012: 23–25.
[2] M E Aminanto, S Sutikno. *Development of Protection Profile and Security Target for Indonesia Electronic ID Card's (KTP-e) Card Reader Based on Common Criteria v3. 1: 2012/SNI ISO/IEC 15408: 2014*. in Advanced Informatics: Concept, Theory and Application (ICAICTA), 2014 International Conference of, IEEE. 2014: 1–6.
[3] AK Darwis, C Lim. *Design and Implementation of e-ktp (Indonesian Electronic Identity Card) Key Management System*. in Advanced Computer Science and Information System (ICACSIS), 2011 International Conference on, IEEE. 2011: 143–146.
[4] NE Tabet, MA Ayu. *Analysing The Security of NFC Based Payment Systems*. in Informatics and Computing (ICIC), International Conference on, IEEE. 2016: 169–174.
[5] S Batool, NA Saqib, MA. Khan. *Internet of Things Data Analytics for User Authentication and Activity Recognition*. in Fog and Mobile Edge Computing (FMEC), 2017 Second International Conference on, IEEE. 2017: 183–187.
[6] N Hakiem, A Mutholib, U Aditiawarman. *Mobile Based Development of A Voter Information Management System (Sipendalih) for the 2014 Indonesian Presidential Election*: Case of indonesian voters in Malaysia. in Information and Communication Technology for The Muslim World (ICT4M). 2014 The 5th International Conference on, IEEE. 2014: 1–4.
[7] M Andriansyah, M Subali, I Purwanto, SA Irianto, RA Pramono. *e-KTP as The Basis of Home Security System Using Arduino UNO*. in Computer Applications and Information Processing Technology (CAIPT), 2017 4th International Conference on, IEEE. 2017: 1–5.
[8] J Cui, D She, J Ma, Q Wu, J Liu. *A New Logistics Distribution Scheme Based on NFC*. in Network and Information Systems for Computers (ICNISC), 2015 International Conference on, IEEE. 2015: 492–495.
[9] NH Harani, AA Arman, RM Awangga. Improving togaf adm 9.1 migration planning phase by itil v3 service transition. Journal of Physics: Conference Series. 2018; 1007(1): 012036.
[10] D Navani, S Jain, M S Nehra. *The Internet of Things (IoT): A Study of Architectural Elements. in Signal-Image Technology & Internet-Based Systems (SITIS).* 2017 13th International Conference on, IEEE. 2017: 473–478.
[11] R Awangga. Sampeu: *Servicing Web Map Tile Service Over Web Map Service to Increase Computation Performance.* in IOP Conference Series: Earth and Environmental Science. IOP Publishing. 2018; 145(1): 012057.
[12] HK¨ostinger, M Gobber, T Grechenig, B Tappeiner, W Schramm. Developing a NFC Based Patient Iden-Tification and Ward Round System for Mobile Devices Using the Android Platform. In Point-of-Care Healthcare Technologies (PHT). *IEEE*. 2013: 176–179.
[13] N Saparkhojayev, A Nurtayev, G Baimenshina. Access Control and Management System Based On NFC-Technology by The Use of Smart Phones as Keys. *Middle-East Journal of Scientific Research*. 2014; 21(7): 1130–1135.
[14] RS Basyari, SM Nasution, B Dirgantara. *Implementation of Host Card Emulation Mode Over Android Smartphone as Alternative ISO 14443a for Arduino NFC Shield*. in Control, Electronics, Renewable Energy and Communications (ICCEREC), 2015 International Conference on, IEEE. 2015: 160–165.
[15] RM Awangga, NS Fathonah, TI Hasanudin. *Colenak: GPS Tracking Model for Post-Stroke Rehabilitation Program Using AES-CBC url Encryption and QR-Code*. in Information Technology, Information Systems and Electrical Engineering (ICITISEE). 2017 2nd International conferences on. IEEE. 2017: 255–260.
[16] M Vaidehi, BJ Rabi. *Design and Analysis of AES-CBC Mode for High Security Applications*. in Current Trends in Engineering and Technology (ICCTET). 2014 2nd International Conference on. IEEE. 2014: 499–502.

[17] R Awangga. Peuyeum: *A Geospatial url Encrypted Web Framework Using Advance Encryption Standard-Cipher Block Chaining Mode*. in IOP Conference Series: Earth and Environmental Science, 2018; 145(1). IOP Publishing: 012055.
[18] SB Venkata, P Yellai, GD Verma, A Lokesh, K Adithya, SSS. Sanagapati. *A New Light Weight Transport Method for Secured Transmission of Data for IOT*. in Advanced Networks and Telecommunications Systems (ANTS), 2016 IEEE International Conference on, IEEE. 2016: 1–6.
[19] P Mittra, N Rakesh. *A Desktop Application of Qr Code for Data Security and Authentication*. in Inventive Computation Technologies (ICICT). International Conference on IEEE. 2016; 2: 1–5.
[20] F Nadeem. A Taxonomy of Data Management Models in Distributed and Grid Environments. *International Journal of Information Technology and Computer Science (IJITCS)*. 2016; 8: 19.
[21] A Celesti, F Tusa, M Villari, and A Puliafito, Three-phase cross-cloud federation model: The cloud sso authentication. In Advances in Future Internet (AFIN), 2010 second international conference on, IEEE. 2010: 94–101.
[22] X Yang, B Nasser, M Surridge, and S Middleton. A business-oriented cloud federation model for real-time applications. Future Generation Computer Systems. 2012; 28(8): 1158–1167.
[23] D Villegas, N Bobroff, I Rodero, J Delgado, Y Liu, A Devarakonda, L Fong, SM Sadjadi, and M Parashar. Cloud federation in a layered service model. *Journal of Computer and System Sciences*. 2012; 78(5): 1330–1344.
[24] T Iimura, H Hazeyama, and Y Kadobayashi. Zoned federation of game servers: a peer-to-peer approach to scalable multi-player online games. in Proceedings of 3rd ACM SIGCOMM workshop on Network and system support for games. ACM. 2004: 116–120.
[25] B Rochwerger, D Breitgand, E Levy, A Galis, K Nagin, IM Llorente, R Montero, Y Wolfsthal, E Elmroth, J Caceres et al. The reservoir model and architecture for open federated cloud computing. *IBM Journal of Research and Development*. 2009; 53(4): 4–1.