

Volume 01, Nomor 02, Desember 2016

ISSN : 2548-1916

Jurnal Teknik Informatika Unika Santo Thomas (JTIUST)



Diterbitkan Oleh :

Program Studi Teknik Informatika Unika Santo Thomas
Jl. Setiabudi No. 479 F Tanjung Sari Medan
Telp. (061) 821061 Fax : (061) 8213269
Email : tekinfo@ust.ac.id

JTIUST	Volume 01	Nomor 02	Halaman 1 - 49	Medan Desember 2016	ISSN 2548-1916
--------	-----------	----------	-------------------	------------------------	-------------------

SERTIFIKAT

Direktorat Jenderal Penguatan Riset dan Pengembangan,
Kementerian Riset, Teknologi, dan Pendidikan Tinggi



Kutipan dari Keputusan Direktur Jenderal Penguatan Riset dan Pengembangan,
Kementerian Riset, Teknologi, dan Pendidikan Tinggi Republik Indonesia
Nomor: 28/E/KPT/2019
Tentang Hasil Akreditasi Jurnal Ilmiah Periode 5 Tahun 2019

Jurnal Teknik Informatika Unika Santo Thomas (JTIUST)

E-ISSN: 26571501

Penerbit: LPPM Universitas Katolik Santo Thomas Medan

Ditetapkan sebagai Jurnal Ilmiah

TERAKREDITASI PERINGKAT 5

Akreditasi berlaku selama 5 (lima) tahun, yaitu
Volume 3 Nomor 1 Tahun 2018 sampai Volume 7 Nomor 1 Tahun 2022

Jakarta, 26 September 2019

Direktur Jenderal Penguatan Riset dan Pengembangan



Dr. Muhammad Dimiyati
NIP. 195912171984021001



[JTIUST] Submission Acknowledgement Eksternal Kotak Masuk x



Tonni Limbong <jurnal.unika@ust.ac.id>
kepada saya ▾

Rab, 18 Mei 16.44 ☆ ↶ ⋮

🌐 Inggris ▾ > Indonesia ▾ [Terjemahkan pesan](#)

[Nonaktifkan untuk: Inggris](#) x

Yoso Adi Setyoko:

Thank you for submitting the manuscript, "Prototipe Teknik Mutual Authentication Untuk Digital Rights Management" to Jurnal Teknik Informatika UNIKA Santo Thomas. With the online journal management system that we are using, you will be able to track its progress through the editorial process by logging in to the journal web site:

Submission URL: <http://ejournal.ust.ac.id/index.php/JTIUST/authorDashboard/submission/1912>

Username: yosoadi

If you have any questions, please contact me. Thank you for considering this journal as a venue for your work.

Tonni Limbong

Jurnal Teknik Informatika UNIKA Santo Thomas

<http://ejournal.ust.ac.id/index.php/HTIUST>



SURAT KETERANGAN TERIMA PAPER

No. 71016/JTIUST/ACC/05.2022

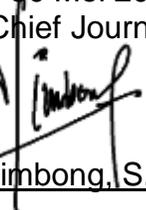
Kepada Yth,
Bapak / Ibu : **Yoso Adi Setyoko, dkk**

di -
Institut Teknologi Telkom Purwokerto

Dengan hormat,
Kami dari Redaksi Jurnal Teknik Informatika UNIKA Santo Thomas (JTIUST) menyampaikan bahwa artikel bapak/ibu dengan judul "**Prototipe Teknik Mutual Authentication Untuk Digital Rights Management**" telah diterima dan sudah direview dan dinyatakan diterima (ACCEPTED) dan akan diterbitkan di **Volume 7 Nomor 1 Edisi Juni 2022**.

Kami mengucapkan terimakasih banyak atas kepercayaan bapak/ibu untuk menerbitkan artikel terbaik bapak di Jurnal kami dan untuk seterusnya kami masih menunggu artikel terbaik bapak berikutnya, kami akan kembali menginformasikan tahap proses berikutnya sampai publish (terbit).

Demikianlah surat keterangan ini kami perbuat untuk dapat dipergunakan sebagaimana perlunya.

Medan, 30 Mei 2022
Editor Chief Journal,

Tonni Limbong, S.Kom, M.Kom



LEMBAR EVALUASI PAPER

Penulis : Yoso Adi Setyoko, dkk
Kode Artikel : JTIUST_71016
Judul : Prototipe Teknik Mutual Authentication Untuk Digital Rights Management

A. OBJEK EVALUASI

Table with 3 columns: No., Deskripsi, and Komentar. It lists 12 evaluation points for the paper, such as originality, relevance, and clarity.

B. KEPUTUSAN REVIEWER

- 1. Artikel dapat diterbitkan secara langsung [...]
2. Artikel dapat diterbitkan dengan sedikit revisi [✓]
3. Artikel dapat diterbitkan dengan banyak revisi [...]
4. Artikel silakan kembali ke kami untuk re-evaluasi setelah revisi [...]
5. Artikel tidak layak untuk diterbitkan berdasarkan alasan di atas [...]

Editor Chief Journal,
Tonni Limbong, S.Kom, M.Kom

PAPER NAME

Paper JTIUST formatting.pdf

AUTHOR

Yoso Adi Setyoko

WORD COUNT

2274 Words

CHARACTER COUNT

14726 Characters

PAGE COUNT

8 Pages

FILE SIZE

276.3KB

SUBMISSION DATE

May 18, 2022 4:34 PM GMT+7

REPORT DATE

May 18, 2022 4:34 PM GMT+7**● 13% Overall Similarity**

The combined total of all matches, including overlapping sources, for each database.

- 10% Internet database
- 6% Publications database
- Crossref database
- Crossref Posted Content database
- 9% Submitted Works database

Prototipe Teknik *Mutual Authentication* Untuk *Digital Rights Management*

Yoso Adi Setyoko¹, Anggi Zafia², Aulia Desy Nur Utomo³

¹Fakultas Informatika Institut Teknologi Telkom Purwokerto

e-mail: ¹yoso@ittelkom-pwt.ac.id, ²zafia@ittelkom-pwt.ac.id,

³auliautomo@ittelkom-pwt.ac.id

Abstrak

Penelitian kami adalah adopsi teknik *mutual authentication* pada *smart card* untuk *Digital Rights Management (DRM)* yang diterapkan menggunakan rekayasa protokol jaringan. Rekayasa protokol tersebut kami adopsi dari teknik *mutual authentication* yang dimiliki oleh *smart card Mifare Desfire*. Pengujian yang dilakukan di penelitian kami adalah pengujian aspek keamanan autentikasi dan kerahasiaan data. Pengujian autentikasi kami lakukan dengan mengubah *master key client* dan *server* yang menentukan keberhasilan autentikasi. Sedangkan pengujian kerahasiaan data dilakukan dengan menyadap data yang dikirim dari *client* ke *server DRM*. Ketika autentikasi oleh *client* dan *server* gagal dilakukan maka perangkat lunak dinyatakan sebagai *software* tidak valid begitu juga sebaliknya. Hasil penelitian kami adalah keberhasilan implementasi adopsi teknik *mutual authentication* milik *smart card* untuk proteksi aplikasi dalam *DRM* mencakup fungsi autentikasi, enkripsi.

Kata kunci— *Prototipe, mutual authentication, DRM, kerahasiaan, rekayasa protokol*

Abstract

Our research is the adoption of *mutual authentication* techniques on *smart cards* for *Digital Rights Management (DRM)* which is applied using *network protocol engineering*. We adopted the *protocol engineering* from the *mutual authentication* technique owned by the *Mifare Desfire smart card*. The tests carried out in our research are testing the security aspects of authentication and data confidentiality. Our authentication test is done by changing the *client* and *server master keys* that determine the success of authentication. Meanwhile, data confidentiality testing is carried out by tapping data sent from the *client* to the *DRM server*. When authentication by the *client* and *server* fails, the *software* is declared invalid and vice versa. The result of our research is the successful implementation of the adoption of the *smart card's mutual authentication* technique for application protection in *DRM* including authentication and encryption functions.

Keywords— *Prototype, mutual authentication, DRM, encryption, protocol engineering*

1. PENDAHULUAN

Penelitian yang kami lakukan saat ini merupakan implementasi dari rancangan protokol keamanan yang kami buat pada penelitian sebelumnya. Penelitian ini dilakukan dengan mengadopsi protokol keamanan yang ada sebelumnya pada *smart card* [1]. Perlu diketahui bahwa kelebihan *smart card* dalam melakukan komunikasi dengan alat pembaca *smart card* menerapkan protokol keamanan secara *offline*. Kemudian kelebihan kedua *smart card* membangun komunikasi aman dengan pembaca tidak menggunakan *Public Key Infrastructure (PKI)* [2]. Oleh sebab itu kami mengadopsi teknik komunikasi aman tersebut untuk keperluan lain di luar penggunaan *smart card* yaitu *Digital Rights Management (DRM)*. Ada perbedaan implementasi *mutual authentication* pada *smart card* dengan implementasi pada penelitian ini yaitu pada penelitian ini kami tidak menggunakan perangkat keras *Secure Access Module (SAM)* untuk penyimpanan kunci privat.

Adapun metode penelitian yang kami terapkan adalah *Design Science Research Methodology (DSRM)*. Tahapan pada *DSRM* terdiri dari identifikasi masalah, menentukan tujuan penelitian,

rancangan, demonstrasi, evaluasi, dan komunikasi. Analisis hasil penelitian yang kami lakukan yaitu bahwa protokol pada *smart card* berhasil diadopsi untuk DRM. Implementasi penelitian kami mencakup beberapa aspek keamanan antara lain aspek autentikasi, aspek kerahasiaan, dan aspek user identitas. Evaluasi hasil penelitian kami adalah penelitian yang kami lakukan terdapat keterbatasan bahwa kunci privat tidak disimpan dalam SAM. Kelanjutan dari penelitian ini adalah penggunaan SAM pada *device* komunikasi.

2. METODE PENELITIAN

20 Bagian dua akan menjelaskan tentang metode penelitian yang dilakukan oleh penulis. Adapun literature review kami meliputi *mutual authentication*, DRM, Philips *mutual authentication*, key diversification, AES, Triple DES, SAM, dan *smart card*. Keterangan lebih detail tentang literatur kami jelaskan sebagai berikut.

6 2.1 Mutual Authentication

Mutual Authentication adalah proses autentikasi yang dilakukan oleh dua buah *device* sebelum melakukan pertukaran data. Studi kasus pada penelitian kami melibatkan dua buah *device* yaitu *client* dan *server*. Mekanisme *mutual authentication* pada penelitian kami adalah *challenge* dan *response*. *Server* melakukan *challenge* kepada *client* dan begitu pula *client* memberikan *challenge* kepada *server*. Jika *challenge* berhasil dijawab maka proses autentikasi berhasil dan jika sebaliknya maka proses autentikasi gagal. Jika proses autentikasi gagal maka komunikasi antar *client* dan *server* tidak bisa dilanjutkan.

2.2 Digital Rights Management (DRM)

Digital Rights Management secara luas mengacu pada seperangkat kebijakan, teknik dan alat-alat yang memandu penggunaan yang tepat dari konten digital [3]. Fungsi utama DRM sangat beragam. Fungsi-fungsi DRM termasuk memfasilitasi pengemasan konten mentah ke dalam bentuk yang sesuai untuk distribusi dan pelacakan yang mudah, melindungi konten untuk transmisi anti rusak, melindungi konten dari penggunaan yang tidak sah, dan memungkinkan spesifikasi hak yang sesuai, yang menentukan mode konsumsi konten. Penelitian kami menggunakan DRM untuk melindungi keaslian perangkat lunak.

2.3 Philips Mutual Authentication

Philips Semiconductors mengeluarkan skema *mutual authentication* yang digunakan pada *smart card*. Skema tersebut sesuai dengan dokumen yang diterbitkan oleh Philips [1]. Skema *mutual authentication* yang dibuat oleh Philips menggunakan kunci privat. Skema tersebut digunakan untuk autentikasi yang bersifat offline antara reader dan *smart card*. Skema tersebut memiliki tiga step untuk *mutual authentication*. Kami mengadopsi mekanisme tersebut untuk implementasi DRM. Hipotesa kami mekanisme ini cocok untuk diterapkan pada DRM karena mampu melindungi perangkat lunak. Selain itu mekanisme *mutual authentication* milik Philips ini merupakan mekanisme protokol yang ringan karena tidak memerlukan algoritma kunci public.

2.4 Key Diversification

Proses pembuatan kunci-kunci baru yang bersifat sementara dari kunci master menggunakan beberapa metode disebut sebagai *key diversification* [4]. Salah satu implementasi *key diversification* yaitu ada pada *smart card*. Dengan adanya *key diversification* maka kunci yang ada pada *smart card* beragam [4]. Kunci pada *smart card* satu dengan *smart card* yang lain akan berbeda-beda. Teknik *key diversification* merupakan langkah pertama yang akan diadopsi pada penelitian kami untuk DRM. Kunci yang akan terbentuk akan beragam untuk masing-masing *client*. Proses *key diversification* menggunakan algoritma AES 128 bit [3][5].

2.5 Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) merupakan algoritma yang digunakan untuk melindungi data elektronik [6]. Algoritma AES merupakan symmetric block cipher yang dapat mengenkripsi dan mendekripsi informasi. Enkripsi adalah proses mengubah data ke dalam bentuk yang tidak dapat dibaca manusia yang disebut sebagai *ciphertext*. Sedangkan dekripsi adalah proses mengkonversi *ciphertext* ke bentuk semula yang dapat dibaca manusia yang disebut sebagai *plaintext*. Algoritma AES dapat diimplementasikan dengan kunci kriptografi berukuran 128, 192, dan 256 bit untuk mengenkripsi dan mendekripsi data dalam blok-blok berukuran 128 bit.

2.6 Triple Data Encryption Standard (Triple DES)

DES merupakan algoritma yang digunakan untuk mengenkripsi data. Triple DES merupakan pengembangan dari Data Encryption Standard (DES) [7]. Menurut skema triple DES merupakan algoritma yang di dalamnya terdiri dari algoritma DES yang digunakan sebanyak tiga kali. Triple DES memiliki skema enkripsi tiga kali menggunakan algoritma DES yang mana masing-masing operasi DES menggunakan kunci yang berbeda-beda. Sehingga triple DES menggunakan tiga kunci.

2.7 Secure Access Module (SAM)

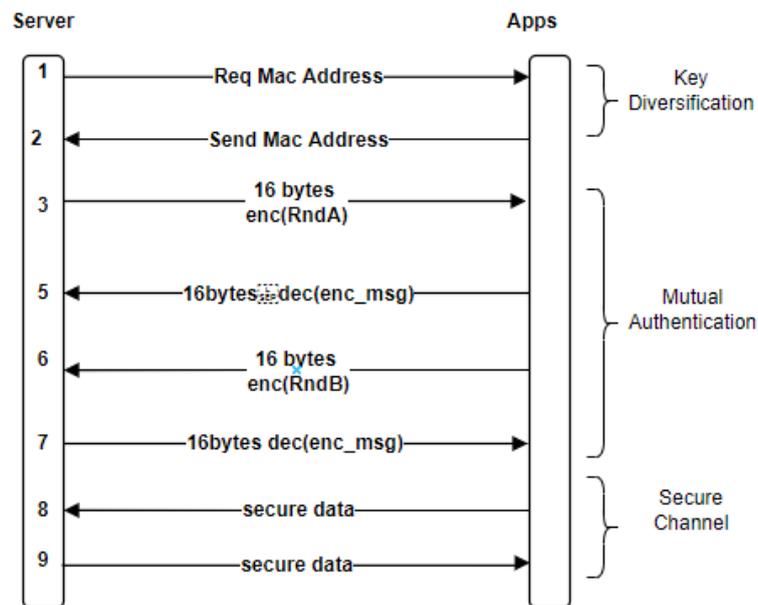
SAM adalah *smart card* yang digunakan untuk meningkatkan keamanan dan performansi kriptografi pada suatu *devices*. Umumnya digunakan pada *device* yang membutuhkan transaksi aman seperti system pembayaran [8]. Contoh system pembayaran yang menggunakan SAM di Indonesia adalah pembayaran dengan transaksi Uang Elektronik (U-nik) untuk bank Mandiri, BRI, BNI, BCA, dan Bank DKI [9]. Namun prototipe penelitian kami saat ini tidak menggunakan perangkat SAM.

15 2.8 Smart Card

Smart Card merupakan sebuah kartu yang memiliki kemampuan komputasi [10]. *Smart card* juga dikatakan memiliki kemampuan kriptografi di dalamnya. *Smart card* digunakan diberbagai keperluan sehari-hari antara lain untuk *Subscriber Identity Module (SIM) Cards*, *financial transactions*, *urban transportation system*, dan *ID cards* [10].

3. HASIL DAN PEMBAHASAN

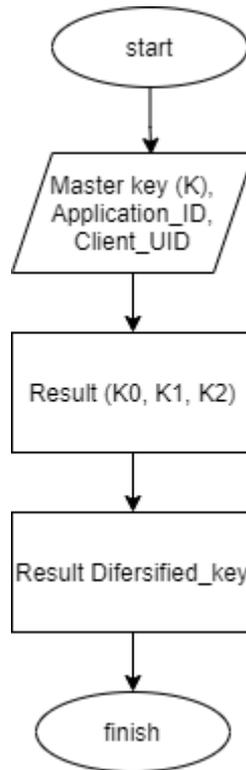
Rancangan protokol yang kami buat terdapat 6 tahap yaitu *key diversification*, *mutual authentication*, *secure message exchange*. Kami mengadopsi juga teknik *key diversification* pada jurnal sebelumnya [1]. Selanjutnya kami mengadopsi Teknik *mutual authentication* yang sebelumnya ada pada *smart card* Philips Mifare Desfire [1]. Kemudian *secure communication* dibangun menggunakan kunci sesi yang dihasilkan pada tahapan sebelumnya. Implementasi protokol keseluruhan dari awal hingga akhir penelitian kami adalah sebagai berikut.



Gambar 1 Skema Protokol Keseluruhan

3.1 Key Diversification

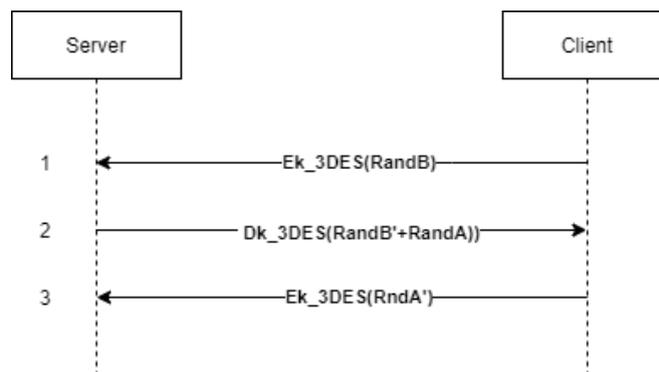
Key diversification merupakan tahap awal dari rekayasa protokol yang kami bangun. Penelitian kami menggunakan teknik *key diversification* yang digunakan pada *smart card* [4][5]. *Key diversification* yang kami coba terapkan adalah sebagai berikut.



Gambar 2 Tahap *Key Diversification*

Tahap *key diversification* di atas menghasilkan sebuah kunci dengan nama *diversified_key* yang selanjutnya digunakan untuk enkripsi dan dekripsi pada proses *mutual authentication*. Algoritma yang digunakan pada proses *key diversification* adalah AES 128 bit. Proses *key diversification* melibatkan application ID dan UID pada *smart card*. Pada penelitian kami application ID dan UID diganti dengan kode unik perangkat keras. Proses *key diversification* ini berdampak pada kunci masing-masing *device* yang menggunakan protokol rancangan kami akan bersifat unik. Perlu diketahui bahwa proses *key diversification* dilakukan oleh kedua belah pihak *client* dan *server*.

3.2 *Mutual Authentication*



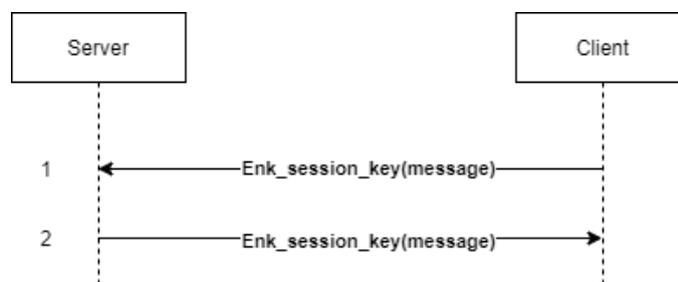
Gambar 3 Tahap 2 *Mutual Authentication*

Sequence diagram di atas adalah proses *mutual authentication*. Ada tiga langkah untuk melakukan *mutual authentication*. Pada langkah nomor 1 *client* memberikan *challenge* kepada *server* dengan mengenkripsi random byte dengan ukuran 8 byte. Kemudian langkah nomor 2 *server* melakukan dekripsi message yang dikirimkan oleh *client* dan mengirimkan ulang pesan *RandB* yang dirotasi kiri dan digabung dengan *RandA* milik *server*. Selanjutnya *client* mengenkripsi pesan dan mendapatkan hasil *RandB'* kemudian *RandB'* dirotasi kanan. Jika hasil rotasi kanan *RandB'* sama dengan *RandB* milik *client* maka autentikasi *server* berhasil dan jika sebaliknya maka *client* menolak komunikasi. Selanjutnya langkah nomor 3 *client* melakukan rotasi kiri *RandA* menjadi *RandA'* kemudian dienkripsi oleh *client*. Hasil enkripsi *RandA'* dikirim ke *server*. Kemudian *server* merotasi kanan *RandA'* dan mencocokkan *RandA* dari *client* dan *RandA* yang dimiliki oleh *server*. Jika *RandA* valid maka *mutual authentication* berhasil. Namun jika *RandA* tidak valid maka proses *mutual authentication* gagal dan *server* menolak komunikasi. Proses *mutual*

authentication akan menghasilkan *session key* yang dapat digunakan untuk proses selanjutnya misalnya untuk komunikasi antar *client* dan *server* secara aman. Kunci sesi yang dibuat adalah kombinasi dari RandA, RandB, RandA', dan RandB'. Kunci sesi yang dihasilkan akan selalu berbeda-beda dan acak ketika *client* dan *server* memulai komunikasi.

Proses *mutual authentication* inilah yang fungsinya diadopsi pada penelitian kami untuk melakukan DRM. Pada DRM pihak *client* maupun *server* dapat melakukan verifikasi dengan proses ini. Perangkat lunak dapat berlaku sebagai *client* DRM yang melakukan *mutual authentication* dengan *server*. Teknik ini dapat menjadi terobosan baru untuk melindungi perangkat lunak dari pembajakan yang sebelumnya hanya menggunakan *serial number*.

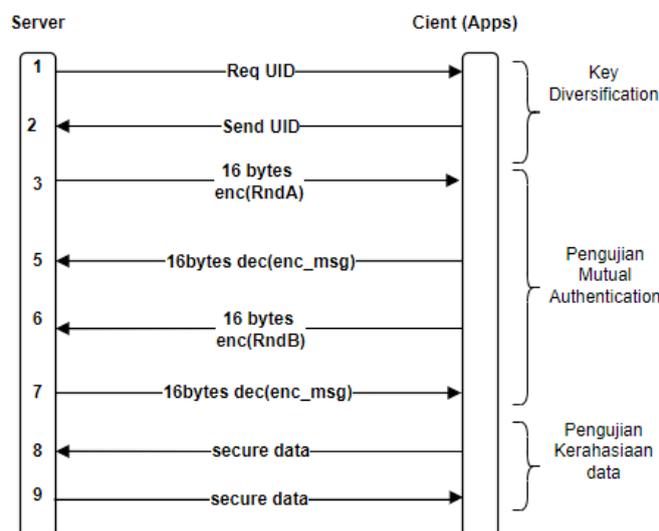
3.3 Secure Communication



Gambar 4 Tahap 3 *Secure Message*

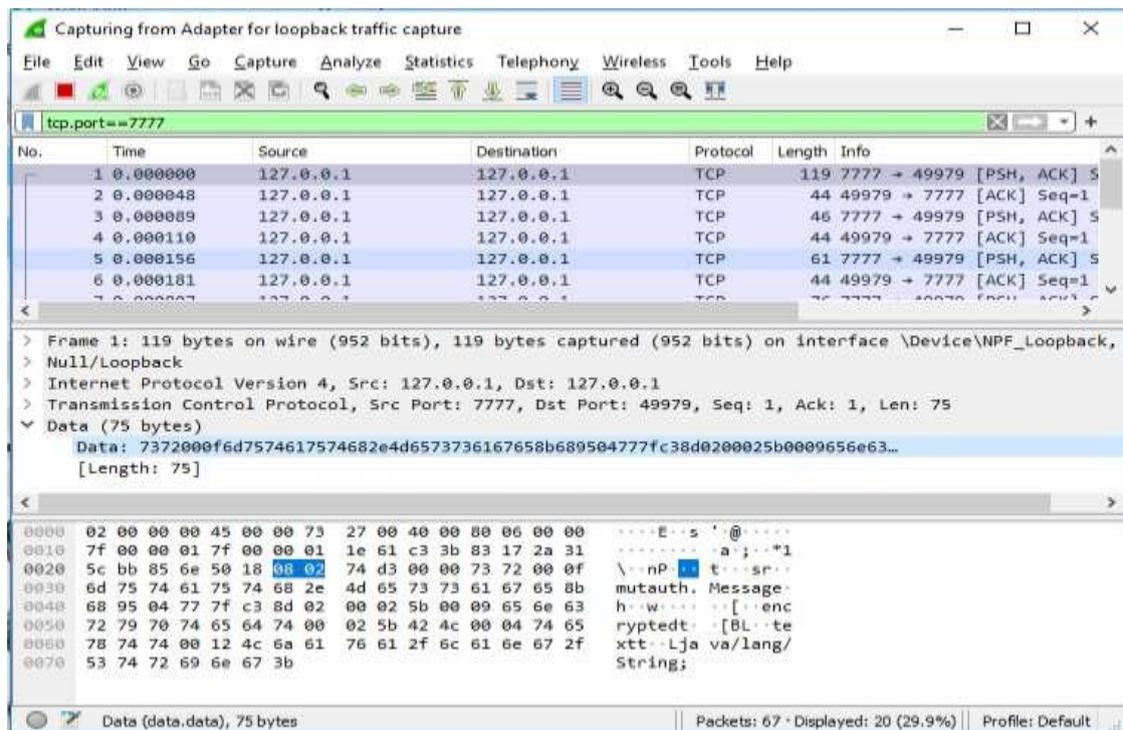
Fungsi ketiga *secure message* merupakan fungsi lanjutan setelah proses *mutual authentication* berhasil. Fungsi DRM ada pada *mutual authentication*. Dengan memanfaatkan kunci sesi yang terbentuk maka *client* dan *server* dapat memanfaatkan kunci sesi untuk bertukar pesan secara aman atau terenkripsi. Pembahasan dan implementasi tentang komunikasi aman melalui adopsi protokol ini akan menjadi bahan penelitian selanjutnya.

3.4 Pengujian Autentikasi



Gambar 5 Pengujian *Key Diversification*, *Mutual Authentication* dan *Secure Message*

Tahap ini merupakan pengujian proses *mutual authentication* (di dalam bingkai warna hijau). Proses pengujian ini dilakukan dengan memasang UID yang berbeda antara *client* dan *server* maka proses *mutual authentication* gagal dilakukan. Hal ini disebabkan karena *key diversification* yang dihasilkan oleh *client* berbeda dengan *server*. Dengan kunci yang berbeda antara *client* dan *server* maka *server* gagal menjawab *challenge* dari *client*. Dengan gagalnya proses *mutual authentication* tersebut maka *client* dan *server* tidak dapat membentuk kunci sesi.



Gambar 6 Pengujian Kerahasiaan Data dengan Wireshark

Tahap pengujian selanjutnya adalah pengujian *secure message* atau *encrypted message*. Pada figure 3 terdapat pada bingkai warna oranye. Kemudian untuk figure 4 di atas merupakan pengujian sadap data menggunakan tool wireshark. Pada figure 4 data terenkripsi ditandai dengan bingkai warna oranye. Dengan tool wireshark kami mencoba menyadap komunikasi antar *client* dan *server*. Kami mendapatkan capture data melalui wireshark dan mendapatkan data yang terenkripsi antara *client* dan *server*. Ini membuktikan bahwa pesan komunikasi antara *client* dan *server* terlindungi oleh enkripsi dan aman.

4. KESIMPULAN

Kami menyimpulkan bahwa penelitian kami berhasil dilakukan sesuai dengan tujuan penelitian yaitu mengadopsi protokol komunikasi *smart card* untuk diterapkan pada DRM. Seluruh tahap protokol *key diversification*, *mutual authentication*, dan *secure communication* telah diimplementasikan dengan baik. Adapun aspek-aspek yang dapat kami capai dalam rekayasa protokol ini yaitu aspek autentikasi, aspek user identity, dan aspek confidentiality. Pengujian kerahasiaan data kami lakukan dengan bantuan tool *wireshark* untuk menyadap komunikasi. Hasil penyadapan komunikasi membuktikan bahwa komunikasi antar *client* dan *server* sudah terenkripsi dan mencapai aspek *confidentiality*. Dengan ini maka rancangan *mutual authentication* untuk DRM pada penelitian kami sebelumnya berhasil diimplementasikan dan diuji. Penelitian kami selanjutnya dari penelitian ini adalah rancangan dan implementasi *secure messaging*. Kemudian kami juga akan mempertimbangkan bagaimana rancangan dan implementasi protokol untuk mengganti fungsi SAM.

DAFTAR PUSTAKA

- [1] M. D. E. S. Fire and C. Stanford, "Mifare ® DES Fire," no. April, 2009.
- [2] S. Goswami, S. Misra, and M. Mukesh, "A Replay Attack Resilient System for PKI Based Authentication in Challenge-Response Mode for Online Application," *Proc. - 2014 3rd Int. Conf. Eco-Friendly Comput. Commun. Syst. ICECCS 2014*, pp. 144–148, 2015, doi: 10.1109/Eco-friendly.2014.104.
- [3] R. Engelberger, M. Fetscherin, and D. Günnewig, "Digital rights management," *Wirtschaftsinformatik*, vol. 47, no. 2, pp. 141–147, 2005, doi: 10.1007/BF03250987.
- [4] Ç. Polat, K. Yildiz, U. C. Çabuk, and G. F. Kılıç, "Providing key diversity for symmetric encryption in Ad-Hoc wireless networks," *2nd Int. Conf. Comput. Sci. Eng. UBMK 2017*, pp. 298–303, 2017, doi: 10.1109/UBMK.2017.8093393.
- [5] NXP, "Symmetric key diversifications," no. March, pp. 1–23, 2010, [Online]. Available: http://www.nxp.com/documents/application_note/AN10922.pdf.
- [6] B. Rothke, "A look at the Advanced Encryption Standard (AES)," *Inf. Secur. Manag. Handbook, Sixth Ed.*, pp. 1151–1158, 2007, doi: 10.1201/9781439833032.ch89.
- [7] A. Biryukov and C. Cannière, "Data encryption standard (DES)," *Encycl. Cryptogr. Secur.*, vol. 3, pp. 129–135, 2006, doi: 10.1007/0-387-23483-7_94.
- [8] Dr. Peter Klein, "Secure Access Module (SAM)," *CardLogic.com*, 2011. <https://www.cardlogix.com/glossary/sam-card-secure-access-module-secure-application-module/>.
- [9] F. Sibarani, "Kartu SAM, Master App yang Dilakukan dengan Sarana & Keadaan Apa Adanya," 2022, [Online]. Available: <https://www.aktualdetik.com/berita/71177/kartu-sam-master-app-yang-dilakukan-dengan-sarana-keadaan-apa-adanya.html>.
- [10] R. Chandramouli and P. Lee, "Infrastructure standards for smart ID card deployment," *IEEE Secur. Priv.*, vol. 5, no. 2, pp. 92–96, 2007, doi: 10.1109/MSP.2007.34.

● **13% Overall Similarity**

Top sources found in the following databases:

- 10% Internet database
- 6% Publications database
- Crossref database
- Crossref Posted Content database
- 9% Submitted Works database

TOP SOURCES

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	aktualdetik.com Internet	1%
2	Hakan Yildiz, Christopher Ritter, Lan Thao Nguyen, Berit Frech, Maria ... Crossref	1%
3	dspace.daffodilvarsity.edu.bd:8080 Internet	1%
4	Universitas Brawijaya on 2018-07-20 Submitted works	<1%
5	Devos, Nicolas, Christophe Ponsard, Jean-Christophe Deprez, Renaud ... Crossref	<1%
6	repository.ittelkom-pwt.ac.id Internet	<1%
7	journal.ugm.ac.id Internet	<1%
8	Faisal Dharma Adhinata, Apri Junaidi. "Gender Classification on Video ... Crossref	<1%

9	adoc.pub	Internet	<1%
10	hdl.handle.net	Internet	<1%
11	Cagri Polat, Umut Can Cabuk, Kadir Yildiz, Gokhan Dalkilic. "Providing k...	Crossref	<1%
12	Ruoyu Huang, Ying Dong, Guangjiu Bao, Yuhong Liu, Ming Wei, Jiaxuan...	Crossref	<1%
13	ieeexplore.ieee.org	Internet	<1%
14	Sriwijaya University on 2019-06-27	Submitted works	<1%
15	id.scribd.com	Internet	<1%
16	P. Frojdh, U. Horn, M. Kampmann, A. Nohlgren, M. Westerlund. "Adapti...	Crossref	<1%
17	docplayer.net	Internet	<1%
18	Universitas Putera Batam on 2021-01-13	Submitted works	<1%
19	dl.gi.de	Internet	<1%
20	scribd.com	Internet	<1%

21	Universitas Brawijaya on 2017-02-15	<1%
Submitted works		
<hr/>		
22	Universitas Atma Jaya Yogyakarta on 2018-01-09	<1%
Submitted works		

LEMBAR
HASIL PENILAIAN SEJAWAT SEBIDANG ATAU *PEER REVIEW*
KARYA ILMIAH : JURNAL NASIONAL TERAKREDITASI

Judul Karya Ilmiah (artikel) : Prototipe Teknik *Mutual Authentication* Untuk *Digital Rights Management*
 Nama Penulis : **Yoso Adi Setyoko**, Anggi Zafia, Aulia Desy Nur Utomo
 Jumlah Penulis : 3
 Status Pengusul : penulis pertama dan korespondensi
 Identitas Jurnal Ilmiah: a. Nama Jurnal : Jurnal Teknik Informatika Unika Santo Thomas (JTIUST)
 b. Nomor ISSN : 2657-1501
 c. Volume, Nomor, Bulan Tahun : Vol 7, No. 1, Juni 2022
 d. Penerbit : LPPM Universitas Katolik Santo Thomas
 e. DOI artikel (jika ada) : -

Kategori Publikasi Jurnal Ilmiah (beri v pada kategori yang tepat)

- Jurnal Ilmiah Nasional Terakreditasi Dikti*
 Jurnal Ilmiah Nasional Terakreditasi Peringkat 1/2/3/4/5/6*

Hasil Penilaian *Peer Review* :

Komponen yang dinilai	Nilai Maksimal Jurnal Ilmiah				Nilai Akhir yang Diperoleh
	Nasional terakreditasi Dikti	Nasional terakreditasi peringkat 1 dan 2	Nasional terakreditasi peringkat 3 dan 4	Nasional terakreditasi peringkat 5 dan 6	
a. Kelengkapan unsur isi artikel (10%)				1,5	1,4
b. Ruang lingkup dan kedalaman pembahasan (30%)				4,5	4,1
c. Kecukupan dan kemutakhiran data /informasi dan metodologi (30%)				4,5	4,5
d. Kelengkapan unsur dan kualitas terbitan/jurnal (30%)				4,5	4,3
Total = 100%				15	14,3
Nilai Pengusul = 60%					8,58

Catatan penilaian artikel oleh Reviewer 1 :

- Kelengkapan dan kesesuaian unsur :
Isi artikel lengkap memuat Title, Author, Abstract, Introduction, Research Method, Result and Discussion, Conclusion and References. Artikel sudah memenuhi persyaratan dan terdapat ISBN serta terakreditasi SINTA
- Ruang lingkup dan kedalaman :
Ruang lingkup dan kedalaman artikel baik. Artikel membahas tentang adopsi protokol autentikasi dari sebuah sistem yaitu produk dari Philips Semiconductor. Artikel secara sistematis membahas protokol autentikasi yang terdiri dari pembangkitan kunci hingga client dan server saling autentikasi.
- Kecukupan dan kemutakhiran data serta metodologi :
Kecukupan kemutakhiran data serta metodologi **mutakhir** saat artikel diterbitkan. Sebagian besar pustaka yang dicantumkan kurang lebih di 5 tahun terakhir.

*Coret yang tidak perlu

4. Kelengkapan unsur kualitas penerbit :
Artikel yang ada di jurnal JTIUST sudah terpublikasi. Jurnal JTIUST sudah dikelola secara OJS dengan DOI jurnal : [10.54367/jtiust.v7i1](https://doi.org/10.54367/jtiust.v7i1)
5. Indikasi Plagiasi : tidak ada unsur plagiasi, hasil similarity rendah yaitu 13 persen
6. Kesesuaian Bidang Ilmu : sudah sesuai dengan bidang ilmu penulis yaitu Ilmu Komputer

29 Juni 2022

Reviewer 1,



Gita Fadila Fitriana, S.Kom., M. Kom

0620039302

Unit Kerja : IT Telkom Purwokerto

Jabatan Fungsional : Lektor

Bidang Ilmu : Teknik Informatika

Prosentase Angka Kredit Penulis untuk :

- **jurnal dan prosiding :**

1. Penulis Pertama sekaligus korespondensi = 60%
2. Terdiri dari : Penulis pertama; Korespondensi; Pendamping
= : 40% ; 40%; 20%
3. Terdiri dari : Penulis pertama; korespondensi = 50% ; 50%

- **Karya ilmiah lain :** Penulis pertama; Pendamping= 60%;40%

LEMBAR
HASIL PENILAIAN SEJAWAT SEBIDANG ATAU *PEER REVIEW*
KARYA ILMIAH : JURNAL NASIONAL TERAKREDITASI

Judul Karya Ilmiah (artikel) : Prototipe Teknik *Mutual Authentication* Untuk *Digital Rights Management*
 Nama Penulis : **Yoso Adi Setyoko**, Anggi Zafia, Aulia Desy Nur Utomo
 Jumlah Penulis : 3
 Status Pengusul : penulis pertama dan korespondensi
 Identitas Jurnal Ilmiah: a. Nama Jurnal : Jurnal Teknik Informatika Unika Santo Thomas (JTIUST)
 b. Nomor ISSN : 2657-1501
 c. Volume, Nomor, Bulan Tahun : Vol 7, No. 1, Juni 2022
 d. Penerbit : LPPM Universitas Katolik Santo Thomas
 e. DOI artikel (jika ada) : -

Kategori Publikasi Jurnal Ilmiah (beri v pada kategori yang tepat)

- Jurnal Ilmiah Nasional Terakreditasi Dikti*
 Jurnal Ilmiah Nasional Terakreditasi Peringkat ~~1/2/3/4/5/6~~*

Hasil Penilaian *Peer Review* :

Komponen yang dinilai	Nilai Maksimal Jurnal Ilmiah				Nilai Akhir yang Diperoleh
	Nasional terakreditasi Dikti	Nasional terakreditasi peringkat 1 dan 2	Nasional terakreditasi peringkat 3 dan 4	Nasional terakreditasi peringkat 5 dan 6	
a. Kelengkapan unsur isi artikel (10%)				1.5	1.4
b. Ruang lingkup dan kedalaman pembahasan (30%)				4.5	4.3
c. Kecukupan dan kemutakhiran data /informasi dan metodologi (30%)				4.5	4.2
d. Kelengkapan unsur dan kualitas terbitan/jurnal (30%)				4.5	4.6
Total = 100%				15	14.5
Nilai Pengusul = 60 %					8,7
Nilai rata-rata Reviewer 1 dan 2					$(8,58+8,7)/2 = 8,64$

Catatan penilaian artikel oleh Reviewer 2 :

- Kelengkapan dan kesesuaian unsur :
Isi artikel **lengkap** dan sesuai unsur artikel yaitu Title, Author, Abstract, Introduction, Research Method, Result and Duscussion, Conclusion and References.
- Ruang lingkup dan kedalaman :
Ruang lingkup dan kedalaman artikel sudah baik. Adopsi protokol autentikasi dari Philips Semikonduktor dapat dilakukan dengan baik. Pembahasan adopsi protokol autentikasi sudah cukup detail dari awal hingga autentikasi berhasil.
- Kecukupan dan kemutakhiran data serta metodologi :
Kecukupan dan kemutakhiran data sudah baik, terlihat dari referensi yang digunakan sebagian besar berasal dari

*Coret yang tidak perlu

jurnal internasional. Sebagian besar referensi yang digunakan adalah artikel yang terbit kurang lebih 5 tahun terakhir.

4. Kelengkapan unsur kualitas penerbit :
Kelengkapan unsur kualitas penerbit sudah **lengkap**. Jurnal terpublikasi dan dikelola secara OJS serta memiliki doi : [10.54367/jtiust.v7i1](https://doi.org/10.54367/jtiust.v7i1).
5. Indikasi Plagiasi :
Hasil pengecekan similarity adalah 13 persen, artinya tidak ada unsur plagiasi.
6. Kesesuaian Bidang Ilmu :
Artikel ini sesuai dengan bidang ilmu penulis yaitu Ilmu Komputer

29 Juni 2022

Reviewer 2,



Aditya Wijayanto, S.Kom., M.Cs

0608118902

Unit Kerja : IT Telkom Purwokerto

Jabatan Fungsional : Lektor

Bidang Ilmu : Ilmu Komputer

Prosentase Angka Kredit Penulis untuk :

- jurnal dan prosiding :

1. Penulis Pertama sekaligus korespondensi = 60%
 2. Terdiri dari : Penulis pertama; Korespondensi; Pendamping
= : 40% ; 40%; 20%
 3. Terdiri dari : Penulis pertama; korespondensi = 50% ; 50%
- Karya ilmiah lain : Penulis pertama; Pendamping= 60%;40%

*Coret yang tidak perlu

Prototipe Teknik *Mutual Authentication* Untuk *Digital Rights Management*

Yoso Adi Setyoko¹, Anggi Zafia², Aulia Desy Nur Utomo³

¹Fakultas Informatika Institut Teknologi Telkom Purwokerto
e-mail: ¹yoso@ittelkom-pwt.ac.id, ²zafia@ittelkom-pwt.ac.id,
³auliautomo@ittelkom-pwt.ac.id

Abstrak

Penelitian kami adalah adopsi teknik *mutual authentication* pada *smart card* untuk *Digital Rights Management (DRM)* yang diterapkan menggunakan rekayasa protokol jaringan. Rekayasa protokol tersebut kami adopsi dari teknik *mutual authentication* yang dimiliki oleh *smart card Mifare Desfire*. Pengujian yang dilakukan di penelitian kami adalah pengujian aspek keamanan autentikasi dan kerahasiaan data. Pengujian autentikasi kami lakukan dengan mengubah *master key client* dan *server* yang menentukan keberhasilan autentikasi. Sedangkan pengujian kerahasiaan data dilakukan dengan menyadap data yang dikirim dari *client* ke *server DRM*. Ketika autentikasi oleh *client* dan *server* gagal dilakukan maka perangkat lunak dinyatakan sebagai *software* tidak valid begitu juga sebaliknya. Hasil penelitian kami adalah keberhasilan implementasi adopsi teknik *mutual authentication* milik *smart card* untuk proteksi aplikasi dalam *DRM* mencakup fungsi autentikasi, enkripsi.

Kata kunci— *Prototipe, mutual authentication, DRM, kerahasiaan, rekayasa protokol*

Abstract

Our research is the adoption of *mutual authentication* techniques on *smart cards* for *Digital Rights Management (DRM)* which is applied using *network protocol engineering*. We adopted the *protocol engineering* from the *mutual authentication* technique owned by the *Mifare Desfire smart card*. The tests carried out in our research are testing the security aspects of authentication and data confidentiality. Our authentication test is done by changing the *client* and *server master keys* that determine the success of authentication. Meanwhile, data confidentiality testing is carried out by tapping data sent from the *client* to the *DRM server*. When authentication by the *client* and *server* fails, the *software* is declared invalid and vice versa. The result of our research is the successful implementation of the adoption of the *smart card's mutual authentication* technique for application protection in *DRM* including authentication and encryption functions.

Keywords— *Prototype, mutual authentication, DRM, encryption, protocol engineering*

1. PENDAHULUAN

Penelitian yang kami lakukan saat ini merupakan implementasi dari rancangan protokol keamanan yang kami buat pada penelitian sebelumnya. Penelitian ini dilakukan dengan mengadopsi protokol keamanan yang ada sebelumnya pada *smart card* [1]. Perlu diketahui bahwa kelebihan *smart card* dalam melakukan komunikasi dengan alat pembaca *smart card* menerapkan protokol keamanan secara *offline*. Kemudian kelebihan kedua *smart card* membangun komunikasi aman dengan pembaca tidak menggunakan *Public Key Infrastructure (PKI)* [2]. Oleh sebab itu kami mengadopsi teknik komunikasi aman tersebut untuk keperluan lain di luar penggunaan *smart card* yaitu *Digital Rights Management (DRM)*. Ada perbedaan implementasi *mutual authentication* pada *smart card* dengan implementasi pada penelitian ini yaitu pada penelitian ini kami tidak menggunakan perangkat keras *Secure Access Module (SAM)* untuk penyimpanan kunci privat.

Adapun metode penelitian yang kami terapkan adalah *Design Science Research Methodology (DSRM)*. Tahapan pada *DSRM* terdiri dari identifikasi masalah, menentukan tujuan penelitian,

rancangan, demonstrasi, evaluasi, dan komunikasi. Analisis hasil penelitian yang kami lakukan yaitu bahwa protokol pada *smart card* berhasil diadopsi untuk DRM. Implementasi penelitian kami mencakup beberapa aspek keamanan antara lain aspek autentikasi, aspek kerahasiaan, dan aspek user identitas. Evaluasi hasil penelitian kami adalah penelitian yang kami lakukan terdapat keterbatasan bahwa kunci privat tidak disimpan dalam SAM. Kelanjutan dari penelitian ini adalah penggunaan SAM pada *device* komunikasi.

2. METODE PENELITIAN

Bagian dua akan menjelaskan tentang metode penelitian yang dilakukan oleh penulis. Adapun literature review kami meliputi *mutual authentication*, DRM, Philips *mutual authentication*, key diversification, AES, Triple DES, SAM, dan *smart card*. Keterangan lebih detail tentang literatur kami jelaskan sebagai berikut.

2.1 Mutual Authentication

Mutual Authentication adalah proses autentikasi yang dilakukan oleh dua buah *device* sebelum melakukan pertukaran data. Studi kasus pada penelitian kami melibatkan dua buah *device* yaitu *client* dan *server*. Mekanisme *mutual authentication* pada penelitian kami adalah *challenge* dan *response*. *Server* melakukan *challenge* kepada *client* dan begitu pula *client* memberikan *challenge* kepada *server*. Jika *challenge* berhasil dijawab maka proses autentikasi berhasil dan jika sebaliknya maka proses autentikasi gagal. Jika proses autentikasi gagal maka komunikasi antar *client* dan *server* tidak bisa dilanjutkan.

2.2 Digital Rights Management (DRM)

Digital Rights Management secara luas mengacu pada seperangkat kebijakan, teknik dan alat-alat yang memandu penggunaan yang tepat dari konten digital [3]. Fungsi utama DRM sangat beragam. Fungsi-fungsi DRM termasuk memfasilitasi pengemasan konten mentah ke dalam bentuk yang sesuai untuk distribusi dan pelacakan yang mudah, melindungi konten untuk transmisi anti rusak, melindungi konten dari penggunaan yang tidak sah, dan memungkinkan spesifikasi hak yang sesuai, yang menentukan mode konsumsi konten. Penelitian kami menggunakan DRM untuk melindungi keaslian perangkat lunak.

2.3 Philips Mutual Authentication

Philips Semiconductors mengeluarkan skema *mutual authentication* yang digunakan pada *smart card*. Skema tersebut sesuai dengan dokumen yang diterbitkan oleh Philips [1]. Skema *mutual authentication* yang dibuat oleh Philips menggunakan kunci privat. Skema tersebut digunakan untuk autentikasi yang bersifat offline antara reader dan *smart card*. Skema tersebut memiliki tiga step untuk *mutual authentication*. Kami mengadopsi mekanisme tersebut untuk implementasi DRM. Hipotesa kami mekanisme ini cocok untuk diterapkan pada DRM karena mampu melindungi perangkat lunak. Selain itu mekanisme *mutual authentication* milik Philips ini merupakan mekanisme protokol yang ringan karena tidak memerlukan algoritma kunci public.

2.4 Key Diversification

Proses pembuatan kunci-kunci baru yang bersifat sementara dari kunci master menggunakan beberapa metode disebut sebagai *key diversification* [4]. Salah satu implementasi *key diversification* yaitu ada pada *smart card*. Dengan adanya *key diversification* maka kunci yang ada pada *smart card* beragam [4]. Kunci pada *smart card* satu dengan *smart card* yang lain akan berbeda-beda. Teknik *key diversification* merupakan langkah pertama yang akan diadopsi pada penelitian kami untuk DRM. Kunci yang akan terbentuk akan beragam untuk masing-masing *client*. Proses *key diversification* menggunakan algoritma AES 128 bit [3][5].

2.5 Advance Encryption Standard (AES)

Advanced Encryption Standard (AES) merupakan algoritma yang digunakan untuk melindungi data elektronik [6]. Algoritma AES merupakan symmetric block cipher yang dapat mengenkripsi dan mendekripsi informasi. Enkripsi adalah proses mengubah data ke dalam bentuk yang tidak dapat dibaca manusia yang disebut sebagai *ciphertext*. Sedangkan dekripsi adalah proses mengkonversi ciphertext ke bentuk semula yang dapat dibaca manusia yang disebut sebagai *plaintext*. Algoritma AES dapat diimplementasikan dengan kunci kriptografi berukuran 128, 192, dan 256 bit untuk mengenkripsi dan mendekripsi data dalam blok-blok berukuran 128 bit.

2.6 Triple Data Encryption Standard (Triple DES)

DES merupakan algoritma yang digunakan untuk mengenkripsi data. Triple DES merupakan pengembangan dari Data Encryption Standard (DES) [7]. Menurut skema triple DES merupakan algoritma yang di dalamnya terdiri dari algoritma DES yang digunakan sebanyak tiga kali. Triple DES memiliki skema enkripsi tiga kali menggunakan algoritma DES yang mana masing-masing operasi DES menggunakan kunci yang berbeda-beda. Sehingga triple DES menggunakan tiga kunci.

2.7 Secure Access Module (SAM)

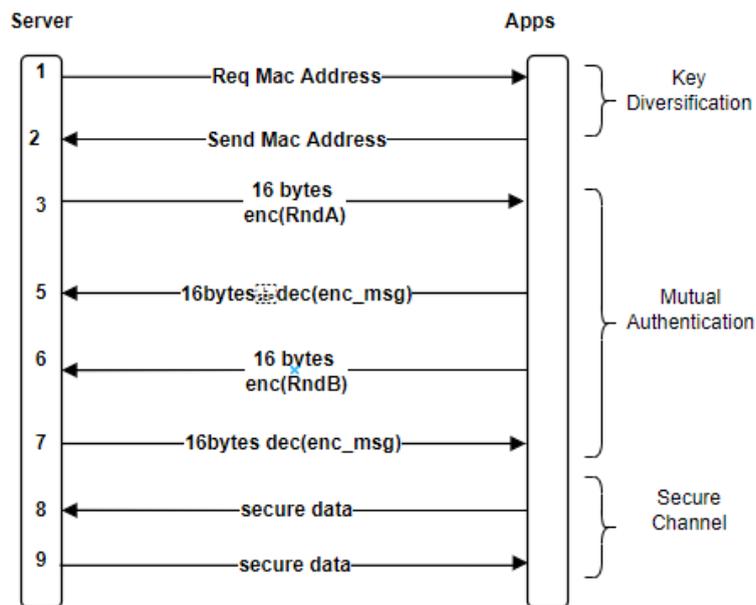
SAM adalah *smart card* yang digunakan untuk meningkatkan keamanan dan performansi kriptografi pada suatu *devices*. Umumnya digunakan pada *device* yang membutuhkan transaksi aman seperti system pembayaran [8]. Contoh system pembayaran yang menggunakan SAM di Indonesia adalah pembayaran dengan transaksi Uang Elektronik (U-nik) untuk bank Mandiri, BRI, BNI, BCA, dan Bank DKI [9]. Namun prototipe penelitian kami saat ini tidak menggunakan perangkat SAM.

2.8 Smart Card

Smart Card merupakan sebuah kartu yang memiliki kemampuan komputasi [10]. *Smart card* juga dikatakan memiliki kemampuan kriptografi di dalamnya. *Smart card* digunakan diberbagai keperluan sehari-hari antara lain untuk *Subscriber Identity Module (SIM) Cards*, *financial transactions*, *urban transportation system*, dan *ID cards* [10].

3. HASIL DAN PEMBAHASAN

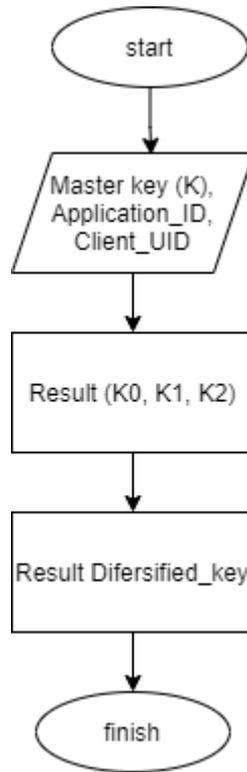
Rancangan protokol yang kami buat terdapat tiga tahap yaitu *key diversification*, *mutual authentication*, *secure message exchange*. Kami mengadopsi juga teknik *key diversification* pada jurnal sebelumnya [1]. Selanjutnya kami mengadopsi Teknik *mutual authentication* yang sebelumnya ada pada *smart card* Philips Mifare Desfire [1]. Kemudian *secure communication* dibangun menggunakan kunci sesi yang dihasilkan pada tahapan sebelumnya. Implementasi protokol keseluruhan dari awal hingga akhir penelitian kami adalah sebagai berikut.



Gambar 1 Skema Protokol Keseluruhan

3.1 Key Diversification

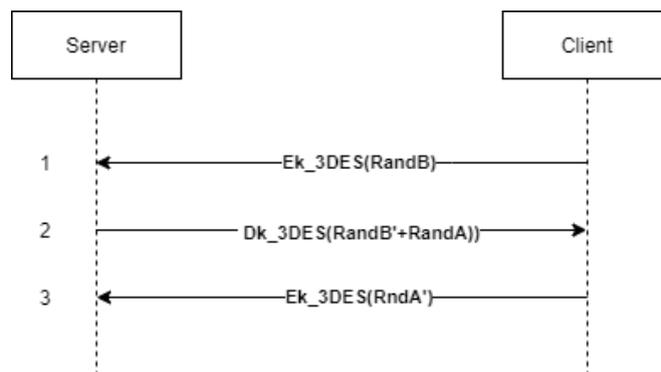
Key diversification merupakan tahap awal dari rekayasa protokol yang kami bangun. Penelitian kami menggunakan teknik *key diversification* yang digunakan pada *smart card* [4][5]. *Key diversification* yang kami coba terapkan adalah sebagai berikut.



Gambar 2 Tahap *Key Diversification*

Tahap *key diversification* di atas menghasilkan sebuah kunci dengan nama *diversified_key* yang selanjutnya digunakan untuk enkripsi dan dekripsi pada proses *mutual authentication*. Algoritma yang digunakan pada proses *key diversification* adalah AES 128 bit. Proses *key diversification* melibatkan application ID dan UID pada *smart card*. Pada penelitian kami application ID dan UID diganti dengan kode unik perangkat keras. Proses *key diversification* ini berdampak pada kunci masing-masing *device* yang menggunakan protokol rancangan kami akan bersifat unik. Perlu diketahui bahwa proses *key diversification* dilakukan oleh kedua belah pihak *client* dan *server*.

3.2 *Mutual Authentication*



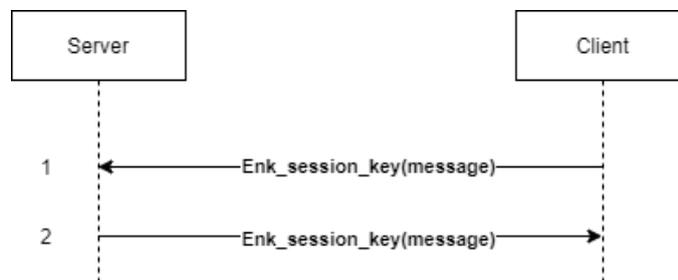
Gambar 3 Tahap 2 *Mutual Authentication*

Sequence diagram di atas adalah proses *mutual authentication*. Ada tiga langkah untuk melakukan *mutual authentication*. Pada langkah nomor 1 *client* memberikan *challenge* kepada *server* dengan mengenkripsi random byte dengan ukuran 8 byte. Kemudian langkah nomor 2 *server* melakukan dekripsi message yang dikirimkan oleh *client* dan mengirimkan ulang pesan *RandB* yang ditorsi kiri dan digabung dengan *RandA* milik *server*. Selanjutnya *client* mengenkripsi pesan dan mendapatkan hasil *RandB'* kemudian *RandB'* dirotasi kanan. Jika hasil rotasi kanan *RandB'* sama dengan *RandB* milik *client* maka autentikasi *server* berhasil dan jika sebaliknya maka *client* menolak komunikasi. Selanjutnya langkah nomor 3 *client* melakukan rotasi kiri *RandA* menjadi *RandA'* kemudian dienkripsi oleh *client*. Hasil enkripsi *RandA'* dikirim ke *server*. Kemudian *server* merotasi kanan *RandA'* dan mencocokkan *RandA* dari *client* dan *RandA* yang dimiliki oleh *server*. Jika *RandA* valid maka *mutual authentication* berhasil. Namun jika *RandA* tidak valid maka proses *mutual authentication* gagal dan *server* menolak komunikasi. Proses *mutual*

authentication akan menghasilkan *session key* yang dapat digunakan untuk proses selanjutnya misalnya untuk komunikasi antar *client* dan *server* secara aman. Kunci sesi yang dibuat adalah kombinasi dari RandA, RandB, RandA', dan RandB'. Kunci sesi yang dihasilkan akan selalu berbeda-beda dan acak ketika *client* dan *server* memulai komunikasi.

Proses *mutual authentication* inilah yang fungsinya diadopsi pada penelitian kami untuk melakukan DRM. Pada DRM pihak *client* maupun *server* dapat melakukan verifikasi dengan proses ini. Perangkat lunak dapat berlaku sebagai *client* DRM yang melakukan *mutual authentication* dengan *server*. Teknik ini dapat menjadi terobosan baru untuk melindungi perangkat lunak dari pembajakan yang sebelumnya hanya menggunakan *serial number*.

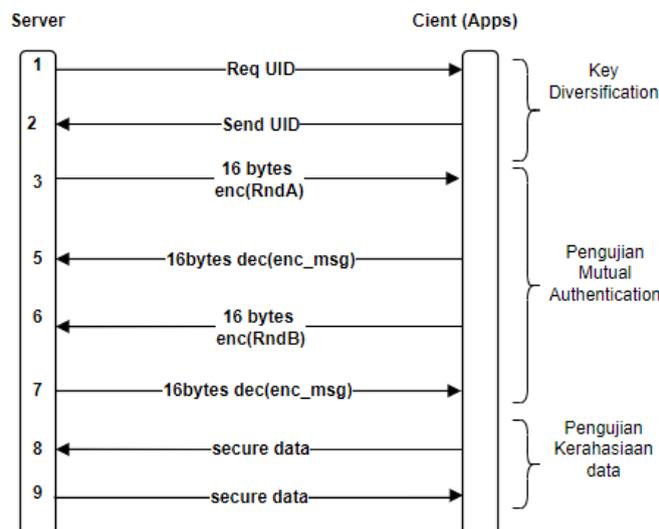
3.3 Secure Communication



Gambar 4 Tahap 3 *Secure Message*

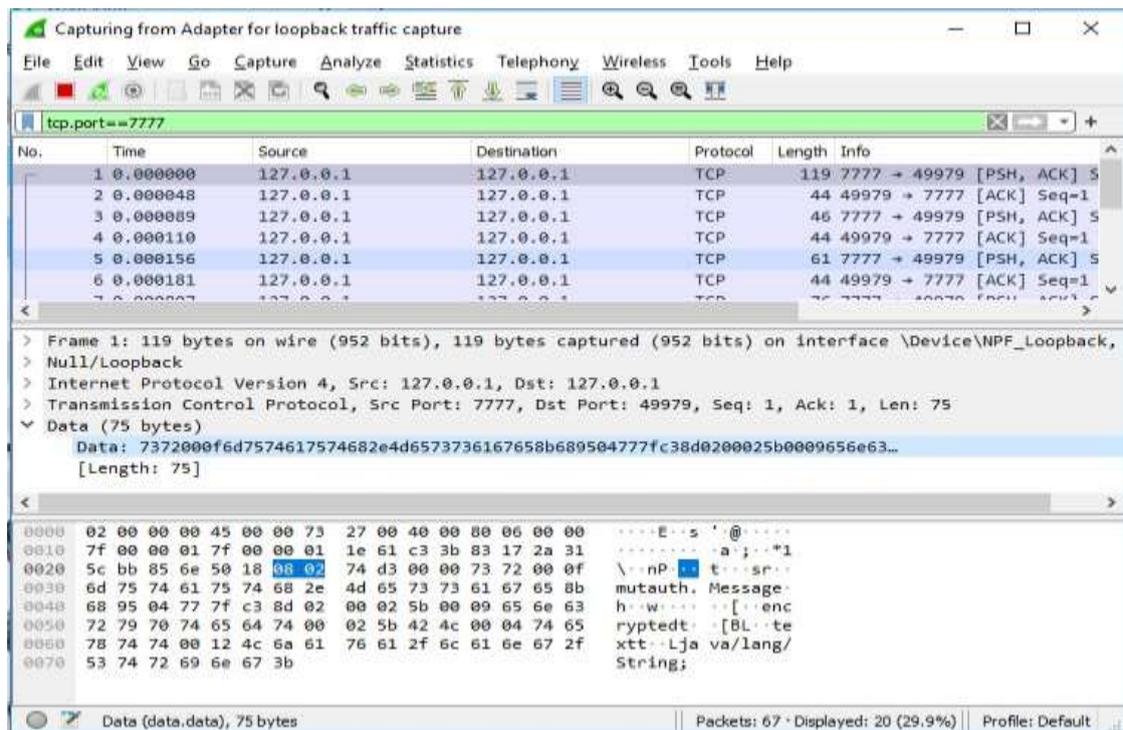
Fungsi ketiga *secure message* merupakan fungsi lanjutan setelah proses *mutual authentication* berhasil. Fungsi DRM ada pada *mutual authentication*. Dengan memanfaatkan kunci sesi yang terbentuk maka *client* dan *server* dapat memanfaatkan kunci sesi untuk bertukar pesan secara aman atau terenkripsi. Pembahasan dan implementasi tentang komunikasi aman melalui adopsi protokol ini akan menjadi bahan penelitian selanjutnya.

3.4 Pengujian Autentikasi



Gambar 5 Pengujian *Key Diversification*, *Mutual Authentication* dan *Secure Message*

Tahap ini merupakan pengujian proses *mutual authentication* (di dalam bingkai warna hijau). Proses pengujian ini dilakukan dengan memasang UID yang berbeda antara *client* dan *server* maka proses *mutual authentication* gagal dilakukan. Hal ini disebabkan karena *key diversification* yang dihasilkan oleh *client* berbeda dengan *server*. Dengan kunci yang berbeda antara *client* dan *server* maka *server* gagal menjawab *challenge* dari *client*. Dengan gagalnya proses *mutual authentication* tersebut maka *client* dan *server* tidak dapat membentuk kunci sesi.



Gambar 6 Pengujian Kerahasiaan Data dengan Wireshark

Tahap pengujian selanjutnya adalah pengujian *secure message* atau *encrypted message*. Pada figure 3 terdapat pada bingkai warna oranye. Kemudian untuk figure 4 di atas merupakan pengujian sadap data menggunakan tool wireshark. Pada figure 4 data terenkripsi ditandai dengan bingkai warna oranye. Dengan tool wireshark kami mencoba menyadap komunikasi antar *client* dan *server*. Kami mendapatkan capture data melalui wireshark dan mendapatkan data yang terenkripsi antara *client* dan *server*. Ini membuktikan bahwa pesan komunikasi antara *client* dan *server* terlindungi oleh enkripsi dan aman.

4. KESIMPULAN

Kami menyimpulkan bahwa penelitian kami berhasil dilakukan sesuai dengan tujuan penelitian yaitu mengadopsi protokol komunikasi *smart card* untuk diterapkan pada DRM. Seluruh tahap protokol *key diversification*, *mutual authentication*, dan *secure communication* telah diimplementasikan dengan baik. Adapun aspek-aspek yang dapat kami capai dalam rekayasa protokol ini yaitu aspek autentikasi, aspek user identity, dan aspek confidentiality. Pengujian kerahasiaan data kami lakukan dengan bantuan tool *wireshark* untuk menyadap komunikasi. Hasil penyadapan komunikasi membuktikan bahwa komunikasi antar *client* dan *server* sudah terenkripsi dan mencapai aspek *confidentiality*. Dengan ini maka rancangan *mutual authentication* untuk DRM pada penelitian kami sebelumnya berhasil diimplementasikan dan diuji. Penelitian kami selanjutnya dari penelitian ini adalah rancangan dan implementasi *secure messaging*. Kemudian kami juga akan mempertimbangkan bagaimana rancangan dan implementasi protokol untuk mengganti fungsi SAM.

DAFTAR PUSTAKA

- [1] M. D. E. S. Fire and C. Stanford, "Mifare ® DES Fire," no. April, 2009.
- [2] S. Goswami, S. Misra, and M. Mukesh, "A Replay Attack Resilient System for PKI Based Authentication in Challenge-Response Mode for Online Application," *Proc. - 2014 3rd Int. Conf. Eco-Friendly Comput. Commun. Syst. ICECCS 2014*, pp. 144–148, 2015, doi: 10.1109/Eco-friendly.2014.104.
- [3] R. Engelberger, M. Fetscherin, and D. Günnewig, "Digital rights management," *Wirtschaftsinformatik*, vol. 47, no. 2, pp. 141–147, 2005, doi: 10.1007/BF03250987.
- [4] Ç. Polat, K. Yildiz, U. C. Çabuk, and G. Dalkiliç, "Providing key diversity for symmetric encryption in Ad-Hoc wireless networks," *2nd Int. Conf. Comput. Sci. Eng. UBMK 2017*, pp. 298–303, 2017, doi: 10.1109/UBMK.2017.8093393.
- [5] NXP, "Symmetric key diversifications," no. March, pp. 1–23, 2010, [Online]. Available: http://www.nxp.com/documents/application_note/AN10922.pdf.
- [6] B. Rothke, "A look at the Advanced Encryption Standard (AES)," *Inf. Secur. Manag. Handbook, Sixth Ed.*, pp. 1151–1158, 2007, doi: 10.1201/9781439833032.ch89.
- [7] A. Biryukov and C. Cannière, "Data encryption standard (DES)," *Encycl. Cryptogr. Secur.*, vol. 3, pp. 129–135, 2006, doi: 10.1007/0-387-23483-7_94.
- [8] Dr. Peter Klein, "Secure Access Module (SAM)," *CardLogic.com*, 2011. <https://www.cardlogix.com/glossary/sam-card-secure-access-module-secure-application-module/>.
- [9] F. Sibarani, "Kartu SAM, Master App yang Dilakukan dengan Sarana & Keadaan Apa Adanya," 2022, [Online]. Available: <https://www.aktualdetik.com/berita/7117/kartu-sam-master-app-yang-dilakukan-dengan-sarana-keadaan-apa-adanya.html>.
- [10] R. Chandramouli and P. Lee, "Infrastructure standards for smart ID card deployment," *IEEE Secur. Priv.*, vol. 5, no. 2, pp. 92–96, 2007, doi: 10.1109/MSP.2007.34.