

Implementasi Tanda Tangan Digital untuk Verifikasi Keaslian Kontrak Pemain Sepak Bola

Salomo Reinhart Gregory Manalu - 13521063

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail : salomo.manalu309@gmail.com

Abstract—Sepak bola menjadi salah satu kegiatan atau olahraga ataupun profesi (di beberapa negara) yang sangat diminati oleh banyak orang. Gaji dan nilai kontrak pemain bola profesional memiliki jumlah yang sangat tinggi. Kontrak dari seorang pemain bola dapat bernilai hingga ratusan juta euro. Karena nilainya yang sangat tinggi dan besarnya peran seorang pemain terhadap suatu klub, keaslian kontrak pemain sepak bola sangatlah penting. Kontrak pemain sepak bola tradisionalnya ditandatangani secara fisik. Penandatanganan secara fisik sangat rentan terhadap pemalsuan dan manipulasi, terutama di era ini teknologi sudah sangat maju. Dengan perkembangan teknologi informasi, digital signature hadir sebagai solusi untuk menjamin keamanan kontrak pemain sepak bola.

Keywords—kontrak pemain sepak bola, digital signature

I. PENDAHULUAN

Sepak bola bukan hanya olahraga, tetapi juga profesi yang diminati di banyak negara di seluruh dunia. Sepak bola adalah profesi yang sangat menguntungkan secara finansial karena sangat populer dan menarik. Pemain sepak bola profesional sering menerima gaji dan kontrak yang sangat tinggi, dengan beberapa kontrak mencapai ratusan juta euro. Nilai kontrak yang sangat tinggi ini menunjukkan betapa pentingnya peran seorang pemain untuk keberhasilan dan prestasi klub sepak bola mereka.

Kontrak pemain sangat penting dalam sepak bola profesional karena menentukan hak dan kewajiban pemain dan klub. Banyak hal termasuk dalam kontrak ini, seperti gaji, bonus, durasi, dan klausul penting lainnya. Oleh karena itu, keaslian dan keabsahan kontrak pemain sangat penting untuk mencegah sengketa hukum dan memastikan semua pihak mematuhi perjanjian.

Kontrak pemain sepak bola biasanya ditandatangani secara fisik. Meskipun demikian, metode penandatanganan fisik memiliki kelemahan yang signifikan, terutama berkaitan dengan kemungkinan pemalsuan dan penyesuaian dokumen. Di era digital saat ini, ketika teknologi informasi berkembang pesat, ada peningkatan risiko terhadap keamanan dokumen. Solusi inovatif untuk masalah ini adalah tanda tangan digital, atau tanda tangan digital, yang menjamin keamanan dan keaslian kontrak pemain sepak bola.

Teknologi kriptografi yang digunakan tanda tangan digital memastikan bahwa dokumen tidak dapat diubah setelah

ditandatangani dan memverifikasi identitas pihak yang menandatangani. Tanda tangan digital memberikan keamanan yang jauh lebih tinggi daripada tanda tangan fisik. Tanda tangan digital dalam kontrak pemain sepak bola meningkatkan keamanan dan menurunkan biaya operasional.

Tujuan dari penelitian ini adalah untuk mempelajari penggunaan tanda tangan digital dalam verifikasi keaslian kontrak pemain sepak bola serta manfaat dan masalah yang mungkin muncul selama adopsi tanda tangan digital. Dengan demikian, penelitian ini diharapkan dapat memberikan manfaat yang signifikan bagi klub sepak bola dan pemangku kepentingan lainnya dalam mengelola kontrak pemain secara lebih aman, efisien, dan kontemporer.

II. DASAR TEORI

A. PDF File

PDF adalah singkatan dari Portable Document Format, sebuah teknologi penformatan dokumen yang dikembangkan oleh Adobe Systems. PDF saat ini menjadi format yang paling umum digunakan untuk berbagi dokumen atau berkas kerja. PDF merupakan format berkas yang biasa digunakan dalam pertukaran dokumen digital di internet. Format PDF berfungsi untuk membuat dan menyimpan dokumen dua dimensi yang terdiri dari teks, huruf, gambar, tautan, dan grafik vektor. Format PDF memastikan bahwa tampilan sebuah dokumen dapat dilihat dan dicetak dalam berbagai sistem operasi komputer secara konsisten dan tidak berubah. Untuk membaca dokumen dengan format PDF, digunakan software atau aplikasi PDF Reader. Ada banyak aplikasi PDF Reader yang tersedia di internet, salah satunya adalah Adobe Acrobat Reader yang disediakan secara gratis oleh Adobe.

B. Kontrak Pemain Sepak Bola

Pemain sepak bola dan klub tempat mereka bermain memiliki hubungan kontraktual. Kontrak adalah komponen penting dalam transaksi bisnis besar dan kecil, baik di dalam negeri maupun di luar negeri. Sangat penting baginya untuk memastikan bahwa seluruh harapan yang tercantum dalam perjanjian yang dibuat oleh para pihak dapat dicapai. Jika ada pelanggaran, ada uang yang harus dibayar. Dengan demikian, kontrak berfungsi sebagai alat untuk menjamin apa yang dapat

dilakukan oleh para pihak dalam sebuah hubungan kerja. Isi dari kontrak pemain sepak bola biasanya mencakup:

1. Durasi Kontrak: Periode waktu di mana pemain akan terikat dengan klub, termasuk tanggal mulai dan berakhirnya kontrak.
2. Gaji dan Bonus: Rincian tentang gaji pokok, bonus penampilan, bonus kemenangan, dan insentif lainnya yang diterima pemain.
3. Hak dan Kewajiban: Tugas dan tanggung jawab pemain serta hak-hak yang mereka miliki, seperti fasilitas kesehatan, asuransi, dan cuti.
4. Klausul Transfer: Ketentuan mengenai transfer pemain ke klub lain, termasuk biaya transfer dan persyaratan lainnya.
5. Klausul Pemutusan Kontrak: Kondisi-kondisi di mana kontrak dapat diakhiri oleh salah satu pihak sebelum waktu yang ditentukan, beserta konsekuensi finansial yang mungkin timbul.
6. Kewajiban Non-olahraga: Kewajiban yang tidak terkait langsung dengan permainan, seperti kehadiran dalam acara promosi klub atau kegiatan sosial.

Premier League
Premier League Contract
Form 20

No.

FA Copy
League Copy
Club Copy
Player Copy

Player's surname	
Player's forename(s)	
Present Postal Address	
Date of Birth	
Place of Birth*	
Nationality	
National Insurance Number	
Club for which Player was last registered	
Club for which Player last played (excluding domestic trials)	

*The Player's birth certificate must be provided to the League in the case of his first registration.

AN AGREEMENT made the (day) _____ day of (month and year) _____

Between _____ Football Club/Company Limited/Plc whose registered office is at (address) _____

Registered Company No _____

(hereinafter referred to as "the Club") of the one part and the above-named Player (hereinafter referred to as "the Player") of the other part

Gambar 1. Kontrak Pemain Sepak Bola EPL

C. Kunci Publik dan Privat Elgamal

Taher ElGamal membuat Algoritma ElGamal pada tahun 1984. Ini awalnya digunakan untuk tanda tangan digital atau tanda tangan digital. Namun, ia diubah sehingga dapat digunakan untuk enkripsi dan dekripsi juga. ElGamal digunakan dalam program GNU, program PGP, dan program keamanan jaringan lainnya. Jika p adalah bilangan prima dan g dan y adalah semua bilangan bulat, maka masalah algoritma diskrit

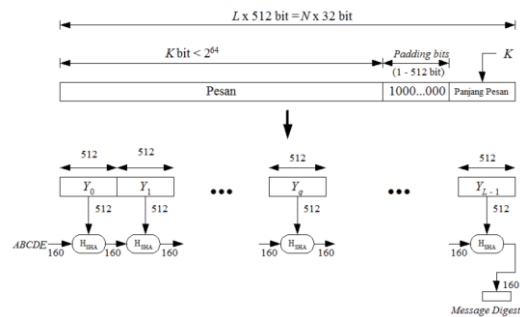
adalah sulitnya menghitungnya. Cari x yang membuat $g^x \equiv y \pmod{p}$.

Besaran - besaran yang digunakan dalam algoritma ElGamal adalah :

1. Bilangan Prima p (Publik)
2. Bilangan acak, g ($g < p$) (Publik)
3. Bilangan acak, x ($x < p-3$) (Privat)
4. $y = g^x \pmod{p}$ (Publik)
5. m (Plainteks) (Privat)
6. a dan b (Ciphertexts) (Publik)

D. Hash SHA-1

SHA adalah fungsi hash satu-arah yang dibuat oleh NIST dan digunakan bersama DSS (Digital Signature Standard). Oleh NSA, SHA dinyatakan sebagai standard fungsi hash satu-arah. SHA didasarkan pada MD4 yang dibuat oleh Ronald L. Rivest dari MIT. Algoritma SHA menerima masukan berukuran maksimum 264 bit (2.147.483.648 gigabyte) dan menghasilkan message digest yang panjangnya 160 bit. Message digest dari SHA lebih panjang dari message digest yang dihasilkan oleh



Gambar 2. Skema SHA-1 Hash

Langkah-langkah dalam pembuatan message digest pada SHA-1 adalah sebagai berikut:

1. Penambahan bit-bit pengganjal (padding bits).
2. Penambahan nilai panjang pesan semula.
3. Inisialisasi penyangga (buffer) MD.
4. Pengolahan pesan dalam blok berukuran 512 bit.

E. Tanda Tangan Digital

Tanda tangan digital adalah mekanisme kriptografi yang digunakan untuk memverifikasi keaslian dan integritas pesan atau dokumen digital. Tanda tangan digital dibuat dengan menggunakan algoritma kriptografi seperti RSA atau DSA yang melibatkan penggunaan kunci publik dan kunci privat. Tanda tangan digital memberikan layanan berupa kerahasiaan pesan, keaslian pesan, otentikasi, dan anti-penyangkalan. Jika tanda-tangan seseorang pada dokumen cetak selalu sama, apa pun isi dokumennya, maka tanda-tangan digital selalu berbeda-beda

antara satu pesan dengan pesan lain, dan/atau antara satu kunci dengan kunci yang lain.

Berbeda dengan tanda tangan fisik yang selalu sama terlepas dari isi dokumennya, tanda tangan digital selalu berbeda-beda untuk setiap pesan yang berbeda dan/atau setiap kunci yang berbeda. Hal ini dikarenakan tanda tangan digital bergantung pada konten spesifik dari pesan atau dokumen yang ditandatangani serta kunci privat yang digunakan untuk membuatnya. Dengan demikian, setiap perubahan kecil dalam pesan akan menghasilkan tanda tangan digital yang berbeda, sehingga memastikan integritas pesan dan memudahkan deteksi modifikasi yang tidak sah.

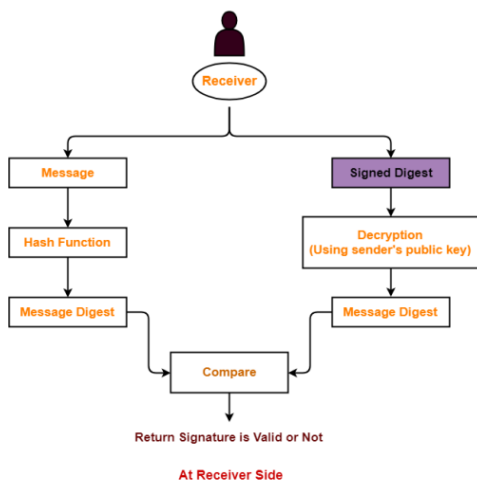
Berikut ini adalah syarat-syarat tanda-tangan digital:

1. Tanda tangan harus berupa rangkaian bit yang bergantung pada pesan yang ditandatangani
2. Tanda tangan harus menggunakan informasi yang unik (=kunci) dari pengirim untuk mencegah pemalsuan dan penyangkalan
3. Membangkitkan tanda tangan digital harus relatif mudah dilakukan
4. Mengenali dan memverifikasi tanda tangan digital harus relatif mudah dilakukan
5. Secara komputasi hampir tidak mungkin memalsukan tanda tangan digital, baik dengan merekonstruksi pesan baru untuk tanda tangan digital yang sudah ada, atau merekonstruksi tanda tangan curang untuk pesan yang diberikan
6. Menyimpan salinan tanda tangan digital ke dalam storage harus mudah dilakukan secara praktek.

Dua proses dalam tanda tangan digital adalah:

1. Penandatanganan (signing)
2. Verifikasi pesan (verification)

Tanda tangan digital juga dapat menggunakan kombinasi pemakaian kunci publik dan privat kriptografi dengan hash functions. Berikut adalah skema kombinasi kunci publik privat kriptografi dengan hash:



Gambar 3. Skema Kombinasi Digital Signature

III. IMPLEMENTASI TANDA TANGAN DIGITAL

A. Deskripsi

Implementasi tanda tangan digital dalam verifikasi keaslian kontrak pemain sepak bola melibatkan serangkaian langkah yang menggunakan teknologi kriptografi untuk memastikan integritas dan keaslian dokumen. Tanda tangan digital memungkinkan kontrak ditandatangani secara elektronik dengan tingkat keamanan yang tinggi, mengurangi risiko pemalsuan dan manipulasi. Langkah-langkah umum dalam proses tanda tangan digital meliputi pembuatan kunci kriptografi, pembuatan hash dari dokumen, dan penggunaan algoritma enkripsi untuk menghasilkan tanda tangan digital yang dapat diverifikasi oleh pihak lain.

B. Implementasi

Proses implementasi tanda tangan digital untuk verifikasi keaslian kontrak pemain sepak bola melibatkan serangkaian langkah teknis yang dirancang untuk memastikan keamanan dan integritas dokumen kontrak. Langkah-langkah ini mencakup pembuatan kunci kriptografi oleh pemain dan klub, pembuatan hash dari dokumen kontrak, enkripsi hash menggunakan kunci privat untuk menghasilkan tanda tangan digital, dan verifikasi tanda tangan digital oleh pihak penerima menggunakan kunci publik.

Berikut langkah-langkah implementasi digital signature pada kontrak pemain sepak bola:

1. Pembuatan kunci publik privat.

Langkah pertama adalah pembuatan sepasang kunci kriptografi, yaitu kunci privat dan kunci publik. Kunci privat digunakan oleh pemain dan klub untuk menandatangani dokumen secara digital, sementara kunci publik digunakan oleh pihak penerima untuk memverifikasi tanda tangan digital tersebut. Pembuatan kunci ini biasanya dilakukan menggunakan algoritma kriptografi seperti RSA atau Elgamal, yang dikenal memiliki tingkat keamanan yang tinggi.

2. Distribusi kunci publik kepada pihak yang membutuhkan verifikasi.

Setelah kunci publik dan privat dibuat, kunci publik harus didistribusikan kepada pihak-pihak yang membutuhkan verifikasi tanda tangan digital, seperti federasi sepak bola, agen pemain, dan pihak terkait lainnya. Distribusi kunci publik ini dilakukan dalam format yang aman, seperti PEM, untuk memastikan bahwa kunci tersebut dapat digunakan untuk verifikasi tanpa risiko penyalahgunaan.

3. Penggunaan algoritma hash.

Langkah berikutnya adalah menggunakan algoritma hash untuk membuat representasi unik dari dokumen kontrak. Algoritma hash seperti SHA-256 menghasilkan nilai hash yang unik untuk setiap dokumen, sehingga setiap perubahan pada dokumen akan menghasilkan nilai hash yang berbeda. Hal ini

penting untuk memastikan bahwa dokumen tidak dapat diubah tanpa terdeteksi setelah ditandatangani.

4. Pembuatan nilai hash.
Proses pembuatan nilai hash melibatkan pembacaan konten dokumen kontrak dan pengaplikasian algoritma hash untuk menghasilkan nilai hash. Nilai hash ini merupakan ringkasan digital dari dokumen yang akan dienkripsi menggunakan kunci privat untuk membuat tanda tangan digital.
5. Enkripsi nilai hash.
Setelah nilai hash dibuat, langkah selanjutnya adalah mengenkripsi nilai hash tersebut menggunakan kunci privat. Enkripsi ini menghasilkan tanda tangan digital yang unik untuk dokumen tersebut. Tanda tangan digital ini dapat diverifikasi oleh pihak lain menggunakan kunci publik yang sesuai, memastikan bahwa dokumen benar-benar ditandatangani oleh pemilik kunci privat dan tidak mengalami perubahan.
6. Penggabungan tanda tangan dengan dokumen
Tanda tangan digital yang dihasilkan kemudian digabungkan dengan dokumen kontrak. Proses ini biasanya dilakukan dengan menambahkan tanda tangan digital ke metadata dokumen, seperti dalam format PDF. Dengan demikian, tanda tangan digital menjadi bagian integral dari dokumen kontrak, yang dapat diverifikasi oleh pihak lain saat dokumen tersebut diakses.
7. Dekripsi tanda tangan digital
Pihak yang menerima dokumen, seperti federasi sepak bola atau agen pemain, akan menggunakan kunci publik untuk mendekripsi tanda tangan digital. Proses dekripsi ini mengembalikan nilai hash asli yang telah dienkripsi, yang kemudian dapat dibandingkan dengan nilai hash yang dihitung dari dokumen yang diterima.
8. Comparing nilai hash
Langkah terakhir adalah membandingkan nilai hash yang didekripsi dengan nilai hash dari dokumen yang diterima. Jika kedua nilai hash cocok, maka dokumen tersebut dianggap asli dan tidak dimodifikasi, dan tanda tangan digital dianggap valid. Proses verifikasi ini memastikan bahwa dokumen kontrak yang ditandatangani secara digital memenuhi standar keamanan dan integritas yang tinggi.

IV. PENGUJIAN DAN ANALISIS

Pengujian akan dilakukan terhadap salah satu jenis kontrak pemain sepak bola yang ada di dunia ini. Kontrak pemain sepak bola yang akan diuji dan dianalisis adalah kontrak pemain sepak bola English Premier League. Kontrak ini berisi berbagai ketentuan penting yang mengatur hubungan antara pemain dan klub, termasuk durasi kontrak, gaji, bonus, hak dan kewajiban pemain, serta klausul transfer dan pemutusan kontrak. Untuk

tujuan pengujian, dokumen kontrak ini disimpan dalam file bernama *contract.pdf*.

Pada awalnya akan dihasilkan private key dan juga public key. Berikut adalah contoh public key.

```
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAsBG9GhqI7xHoUtsOaaoKOkdrHN4K
RRWVbgJjutLncfYmBI+VhDYVb3hUAbSGNqGD
GwWcbzm8KwKa+v8Vjj7exz3PvzM/64fbDZVH
oY6ZYp2MxSn+t9N+rTpfw5dSJmSI/897Zt2v
tHkYX3+PNRLjSQ/MVycW3Qwc+jExKs/xs+NT
Wp4kCRGMpjPcKkU3yHiilVvREfp+MqDbKK7
QK3x
```

Dan berikut ini adalah private key-nya.

```
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBCkw
ggSjAgEAAoIBAQCwEb0aGojvEehS2w5p6go6
R2sc3gpFFZVuAmO60udx9gxsj5WENhVveFQB
tIY2oYmBzXvObwrApr6/xWOPt7HPc+/Mz/r
h9sNlUehjplinYzFKf63036tOl/Dl1ImZIJ/
z3tm3a+0eRhff481EuNJD8xXJxbdDBz6MTEq
z/Gz41NaniQJEYymOkKQrBTfIEKKVW9ER+n4
yoNsortArfe/sdiFCATnhxhTLZEDw6Nm3P8E
6vQTuPpklyYYPAS7bTDqaGLY84zLNhk3BLLG
BNCbAC/B3R1DnQ3KCwZWTirI2jCYynj4VRfk
GoZayBpJazK3K0PMozKhXSaVeP5//WOpAgMB
AAECggEABLh8gDSaUyaaosckZ/2ietUis92A
+WLwsXL9OBHWEUp48AEAuopgcC9nQbwuNuZ+
nsm4MSYr3bW/TmhqtM20uaqx/sV/mKLW+9SU
3QNuoCxze/etaUHNrk6I2l7piF1SGr+YO+Cv
M0DML+Tk6kCjuSLCCicZTpCVtgsGZshR+L7m
JfxGy3j176YB662f1R0mTkzNrYEBxVPeVd6C
B5o02jDyztNhVnqDutPdfB5NTq5GasKI0WsO
bkisSkBpecnzvJqkqhLEzNuyHhQz8Jpi3aSL
YOoHCYoq/L4njGSNQizxpilxFOJ6KI7u7BRt
8p62I2Utx6BESNnd+et2hajfLQKBgQDzUHxA
nbyS3uJ0wnLiH2DTJkqym4thqscDSb7Cp0ij
b91+v5mvkGb+GcL6J/vu6r75apXDaWNkzQuo
nSvbEUOCsA8L2qZaKfZSsqzTeMTVcjaEtw8b
7PzLOWfGXHP4KPGp1PT03aztt6hZcKIbt63M
XXZ270T7fDDSpFbTFAwj8wKBgQC5P7vPT8Dk
rjllztVy4y6GmmrqqkutqPLkZpoNVGmUVEhi
SCPsRL3MilNXBMyTvF60XCiXmUSpdpJdAxri
9JzEh8HPdWyRr14D2OLDp+aEKem3nJo+PgrM
78rsTtgVJa6k8lXawMBpSreUvhGwz6tv7lzk
t4+N9dwHpe++knCs8wKBgQC4YkXGscI1irIR
yUlGEoFNgbczosX9PW2TEE9/M0XY101FH+1X
HhbueJdI+wPwCfsVdhZv/20/QiOT04eYe3yt
jL3aPdfSe/ouq5ERMHP5TJQD/rV0
```

Setelah pembuatan kunci public dan kunci private, akan dilakukan penggunaan algoritma hash. Algoritma hash ini akan digunakan untuk membuat hash dari data *contract.pdf*.

Berikut ini adalah hasil dari algoritma hash256 terhadap kontrak pemain sepak bola tersebut.

```
Document      Hash      (original) :
fc1ee70622bed80fc94d82e3ed613304620f
647ffcb6769fadc4b0867a7592ea
```

Selanjutnya, hasil dari hash ini akan dilakukan enkripsi. Proses enkripsi ini menggunakan kunci privat yang telah dibuat sebelumnya. Enkripsi hash adalah langkah penting dalam proses tanda tangan digital, karena memastikan bahwa nilai hash tersebut unik dan tidak dapat diubah tanpa deteksi. Dengan mengenkripsi hash menggunakan kunci privat, kita memastikan bahwa hanya pemilik kunci privat yang dapat menghasilkan tanda tangan digital tersebut. Pihak penerima yang memiliki kunci publik dapat memverifikasi tanda tangan digital ini dengan mendekripsi nilai hash yang dienkripsi dan membandingkannya dengan hash yang dihitung dari dokumen yang diterima. Jika kedua nilai hash cocok, dokumen dianggap asli dan tidak dimodifikasi sejak ditandatangani.

Berikut adalah hasil dari enkripsi hashed document.

```
Signature:
0f16202c9134ca5880a83a6227257104b63f
7d3a916d60f190d1ad5eb718a713c9bdb099
3d3e7945a6307dc073cc7566ad9090591ab3
f08ec2f24a85f1896fdf0aeab09b6eec3f36
0be8080e7ca59b32688714206629d04c29b1
381c9153d14d60c44df15f9c4b65e27fe736
79662b54acc9f5d6f4af0f69bac82dfd05ec
017c414ca96660f3dcc8271cf8a6066bb84a
a6f26933cf841bad149475b270fb3c327da8
57ac7fa74df97d687823434f7841d31ebcff
605623de0fcb2cd571cc86d38ad0546c2865
0003d70bc757e6420d905cb4fc29c2ad4af9
28f8efdbb38b99a80d196b7385464bde2af
c91c5e3507d7bf8186aceda3ea71526dd132
c21d45e6
```

Setelah hasil hash dienkripsi dengan kunci privat untuk menghasilkan tanda tangan digital, langkah selanjutnya adalah penggabungan data. Dalam konteks ini, penggabungan data berarti menyatukan dokumen kontrak asli dengan tanda tangan digital yang telah dihasilkan. Tanda tangan digital ditambahkan ke dokumen sebagai metadata atau elemen yang dapat dikenali dan diverifikasi oleh perangkat lunak yang sesuai. Proses ini memastikan bahwa dokumen kontrak yang asli kini memiliki tanda tangan digital yang terikat erat dengan kontennya. Dengan penggabungan ini, setiap kali dokumen dibuka, perangkat lunak dapat mengekstrak tanda tangan digital, mendekripsinya menggunakan kunci publik, dan membandingkan nilai hash yang dihasilkan dari dekripsi dengan hash dokumen yang diterima. Jika nilai-nilai ini sesuai, maka keaslian dan integritas dokumen dapat dipastikan.

Berikut ini adalah kode untuk attach hash pada dokumen

```
def attach_signature_to_pdf(file_path, signature,
output_path):
    pdf_writer = PdfWriter()
    pdf_reader = PdfReader(file_path)

    for page_num in
range(len(pdf_reader.pages)):
        pdf_writer.add_page(pdf_reader.pages[page_num])

    pdf_writer.add_metadata({
        '/Signature': signature.hex()
    })

    with open(output_path, "wb") as f:
        pdf_writer.write(f)
```

Selanjutnya, proses dekripsi tanda tangan digital dilakukan untuk memverifikasi keaslian dokumen. Dekripsi ini dilakukan dengan menggunakan kunci publik yang telah didistribusikan sebelumnya. Ketika tanda tangan digital didekripsi, nilai hash asli yang dienkripsi dengan kunci privat akan diperoleh. Langkah ini memastikan bahwa tanda tangan digital benar-benar berasal dari pemilik kunci privat dan tidak dapat dipalsukan oleh pihak lain. Setelah nilai hash asli didekripsi, tahap berikutnya adalah comparing nilai hash. Dalam tahap ini, nilai hash yang dihasilkan dari dekripsi tanda tangan digital dibandingkan dengan nilai hash yang dihitung langsung dari dokumen yang diterima. Jika kedua nilai hash tersebut cocok, maka dapat dipastikan bahwa dokumen tersebut tidak mengalami perubahan sejak ditandatangani. Proses ini memberikan kepastian bahwa dokumen kontrak pemain sepak bola adalah asli dan tetap utuh, serta bahwa tanda tangan digital benar-benar berasal dari sumber yang sah.

```
Document Hash (original): fc1ee70622bed80fc94d82e3
Document Hash (new): debbc4a0b5dbb6618f85b107637de
Signature: 0f16202c9134ca5880a83a6227257104b63f7d3
1381c9153d14d60c44df15f9c4b65e27fe73679662b54acc9f
fcb2cd571cc86d38ad0546c28650003d70bc757e6420d905cb
Apakah tanda tangan digital valid? True
```

Implementasi tanda tangan digital untuk verifikasi keaslian kontrak pemain sepak bola memberikan beberapa keuntungan signifikan. Pertama, penggunaan kunci kriptografi dan enkripsi hash meningkatkan keamanan dokumen secara drastis, mengurangi risiko pemalsuan dan manipulasi. Kedua, proses ini memastikan bahwa hanya pihak yang sah dengan akses ke kunci privat yang dapat menghasilkan tanda tangan digital yang valid. Ketiga, verifikasi menggunakan kunci publik memungkinkan pihak penerima untuk dengan mudah memeriksa keaslian dan integritas dokumen. Dalam pengujian terhadap kontrak pemain sepak bola English Premier League, hasil menunjukkan bahwa dokumen yang ditandatangani secara digital dapat diverifikasi dengan tingkat keandalan yang tinggi, menjamin bahwa dokumen tidak dimodifikasi sejak penandatanganan. Implementasi ini tidak hanya meningkatkan efisiensi administrasi tetapi juga memberikan jaminan hukum yang kuat,

menguntungkan bagi klub, pemain, dan semua pemangku kepentingan yang terlibat. Dengan demikian, adopsi tanda tangan digital merupakan langkah penting menuju pengelolaan kontrak yang lebih modern dan aman dalam industri sepak bola profesional.

V. KESIMPULAN

Implementasi tanda tangan digital untuk verifikasi keaslian kontrak pemain sepak bola menawarkan solusi yang aman, efisien, dan dapat diandalkan untuk mengatasi tantangan yang terkait dengan pemalsuan dan manipulasi dokumen dalam industri olahraga profesional. Dengan menggunakan teknologi kriptografi seperti kunci privat dan publik serta algoritma hash, tanda tangan digital memastikan bahwa dokumen kontrak tetap utuh dan asli sejak saat penandatanganan hingga verifikasi. Proses ini tidak hanya memperkuat integritas dan autentisitas kontrak, tetapi juga meningkatkan efisiensi administrasi dan memberikan kepastian hukum yang lebih kuat bagi semua pihak yang terlibat.

Pengujian terhadap kontrak pemain sepak bola English Premier League menunjukkan bahwa dokumen yang ditandatangani secara digital dapat diverifikasi dengan mudah dan akurat, memastikan bahwa tidak ada perubahan yang terjadi setelah penandatanganan. Ini memberikan rasa aman baik bagi klub maupun pemain, serta memfasilitasi transparansi dan kepercayaan dalam hubungan kontraktual.

Secara keseluruhan, adopsi tanda tangan digital dalam pengelolaan kontrak pemain sepak bola merupakan langkah maju yang signifikan. Teknologi ini tidak hanya mengurangi risiko dan meningkatkan keamanan, tetapi juga menciptakan kerangka kerja yang lebih modern dan efisien dalam industri sepak bola profesional. Oleh karena itu, penggunaan tanda tangan digital sangat direkomendasikan untuk memastikan keaslian dan integritas kontrak dalam lingkungan yang semakin digital dan global.

UCAPAN TERIMA KASIH

Penulis mengucapkan Syukur kepada Tuhan Yang Maha Esa atas segala rahmatnya sehingga penulis dapat menyelesaikan

makalah kriptografi ini dengan baik. Penulis juga mengucapkan terima kasih yang sebesar-besarnya kepada orang tua, teman, dan juga semua orang yang telah berkontribusi dalam pembuatan makalah ini. Penulis juga secara khusus mengucapkan terima kasih yang sebesar-besarnya kepada Bapak Dr. Ir. Rinaldi Munir, M.T. selaku dosen pengajar Mata Kuliah IF4020 Kriptografi Tahun Ajaran 2023/2024 yang telah mengajarkan berbagai pengetahuan sehingga penulis dapat membuat dan menyelesaikan makalah ini.

REFERENSI

- [1] G Munir R. Kriptografi. 2024.
- [2] <https://www.merdeka.com/trending/apa-itu-pdf-ketahui-definisi-hingga-berbagai-cara-menggunakannya-kln.html>. 2024
- [3] Suprajogi, Agus. Analisis Kontrak Pemain Sepakbola Profesional Serta Kontrak Pinjaman Pemain Berdasarkan Hukum Ketenagakerjaan dan Hukum Perdata. 2024
- [4] T. A. Faizal M., S Arif. Penyusunan Perjanjian Kerja Antara Pemain Sepak Bola Profesional Dengan Klub Persis Solo. 2024

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 12 Juni 2024



Salomo Manalu, 13521063