Kerekayasaan Modul Penjamin Keabsahan Data Medis pada Inovasi Sistem Telemedicine BPPT

Tahar Agastani, Muhammad Iqbal, A. A. N. Ananda Kusuma, Christian W. Purnaadi
Pusat Teknologi Elektronika (PTE)
Badan Pengkajian dan Penerapan Teknologi (BPPT)
Gedung Teknologi 3, Kawasan Puspiptek, Tangerang Selatan 15314, Indonesia
{tahar.agastani, muhammad.iqbal5607, ngurah.ananda, christian.wisnu}@bppt.go.id

***Abstrak* — Telemedicine adalah sistem layanan kesehatan yang memanfaatkan infrastruktur TIK (Teknologi Informasi dan Komunikasi) untuk mengatasi kendala jarak dan waktu dalam penyelenggaraan layanan kesehatan. Salah satu implementasi telemedicine adalah tele-ECG(*Electrocardiology*) di mana kondisi kesehatan jantung pasien direkam oleh dokter umum di fasilitas layanan kesehatan primer, dan kemudian dianalisa oleh dokter spesialis di rumah sakit rujukan. Hasil analisa dokter spesialis selanjutnya digunakan untuk menentukan tindakan pengobatan selanjutnya. Mekanisme kerja seperti ini, di mana data dan analisa medis disimpan secara elektronik dan dikirim melalui jaringan komunikasi publik, memerlukan langkah-langkah pengamanan. Untuk mengatasi potensi sengketa di masa depan, data dan analisa medis harus dijamin keabsahannya menggunakan tanda tangan digital dari pihak-pihak yang bertanggung jawab memberikan layanan kesehatan. Makalah ini memaparkan implementasi tele-ECG yang menyertakan modul tanda tangan digital yang diterapkan pada data medis ECG dalam standar DICOM dan pada analisa medis dalam format PDF. Beberapa uji fungsional dilakukan dalam skenario di mana data mengalami modifikasi, dan sistem dapat memverifikasi keabsahan data dan analisa medis tersebut.**

Keywords—telemedicine, security, digital signatures, PKI (Public Key Infrastructure), ECG, DICOM

I. PENDAHULUAN

Terciptanya kehidupan sehat dan sejahtera untuk setiap individu pada tahun 2030 menjadi target ketiga dalam *Sustainable Development Goals* (SDGs) yang dicanangkan oleh Perserikatan Bangsa-Bangsa [3]. Hal ini merupakan tantangan untuk negara berkembang seperti Indonesia yang sedang intensif membangun berbagai infrastrukur, salah satunya untuk layanan kesehatan. Kondisi geografis dan demografis Indonesia yang heterogen juga mempersulit penyediaan layanan kesehatan berkualitas yang seragam. Diharapkan perkembangan TIK (Teknologi Informasi dan Komunikasi) dapat memberikan solusi atas berbagai kendala di atas. Untuk itu pengembangan infrastruktur informasi harus juga menjadi prioritas selain infrastruktur fisik.

Inovasi sistem telemedicine memungkinkan layanan medis jarak jauh dengan menggunakan infrastruktur jaringan komunikasi dan teknologi informasi. Layanan medis jarak jauh dapat diimplementasikan dengan media transmisi internet, radio, hingga satelit. Penggunaan sistem telemedicine terbukti mampu meningkatkan kepuasan pelayanan serta keterjangkauan akses kesehatan hingga ke daerah terdalam suatu wilayah [8][11]. Melihat prospek pemanfaatannya di Indonesia, maka PTE-BPPT juga melakukan inisiatif untuk mengembangkan sistem telemedicine, yang mana untuk tahap awal difokuskan pada tele-ECG dan tele-Consultation [2] .

Data informasi rekam medis seseorang termasuk ke dalam informasi sensitif dan rahasia yang seharusnya dijaga dari oknum pengguna yang tidak memiliki otoritas. Pada sistem telemedicine, keamanan dan privasi data menjadi faktor penting yang perlu diperhatikan lebih seksama. Tiga unsur penting dari keamanan informasi adalah kerahasiaan (*confidentiality*), integritas data (*integrity*), dan ketersediaan (*availability*) [13]. Kerahasiaan adalah unsur informasi yang hanya dapat diakses oleh pihak yang memiliki otoritas terhadap informasi tersebut. Integritas memiliki definisi unsur yang memastikan bahwa kualitas, keutuhan, dan kelengkapan informasi tetap terjaga. Ketersediaan memastikan bahwa pihak yang memiliki otoritas terhadap informasi dan memiliki hak akses terhadap informasi dapat mengakses informasi tersebut tanpa adanya gangguan maupun hambatan. Ketiga aspek keamanan perlu diterapkan dalam sistem telemedicine untuk memastikan keabsahan data rekam medis pasien agar terpercaya dan dapat dipertanggungjawabkan.

Makalah ini memaparkan inovasi telemedicine BPPT untuk layanan tele-ECG dengan penekanan pada aspek penjaminan keabsahan data dan analisa medis ECG. Pada bagian II dipaparkan gambaran umum inovasi telemedicine BPPT, kemudian dilanjutkan di Bagian III dengan pembahasan tanda tangan dan sertifikat digital di kalangan medis. Bagian IV menjelaskan integrasi modul penjamin keabsahan data pada sistem telemedicine BPPT, dan hasil-hasil uji coba ditunjukkan pada Bagian V.

II. INOVASI SISTEM TELEMEDICINE

Inovasi sistem telemedicine di BPPT telah dilakukan mulai dari tahun 2016 dengan mengembangkan sistem teknologi informasi yang mengintegrasikan alat kesehatan ke dalam satu mesin yang disebut "telemedicine cart". Telemedicine cart akan terhubung dengan server pusat telemedicine yang dapat di implementasikan pada *on premise* maupun di *cloud*. Gambaran besar sistem telemedicine yang dikembangkan di BPPT ditunjukkan pada Fig. 1.

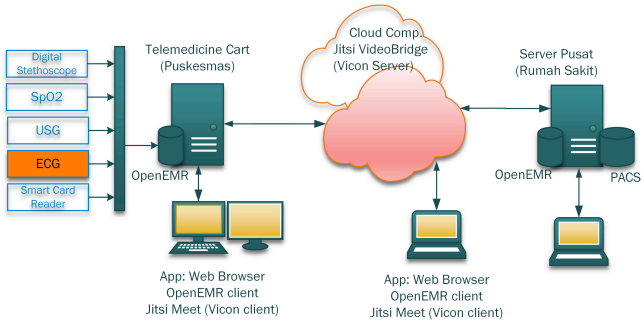

Fig. 1. Gambaran Besar Sistem Telemedicine.

Telemedicine cart menjadi bagian yang terpasang di sisi pasien di Puskesmas dan berfungsi sebagai perangkat *aggregator* menghubungkan berbagai peralatan medis dan berbagai perangkat pendukung lainnya yang diperlukan, misal pembaca kartu cerdas. Aggregasi berbagai perangkat medis memungkinkan sistem untuk menggunakan protokol transport yang seragam untuk berbagai aplikasi medis [10]. Sistem yang saat ini dikembangkan disiapkan untuk perangkat ECG, USG, *vital signs*, dan pembaca kartu cerdas untuk membaca KTP-el.

Supaya data rekam medis dapat dipahami oleh seluruh subsistem, format standar yang dipilih untuk pengiriman dan penyimpanan adalah DICOM (*Digital Imaging and Communications in Medicine*). Standar ini umum digunakan untuk penyimpanan dan pengiriman citra medis (*medical imaging*) seperti: citra Rontgen, MR, CT, *ultrasound* dan lain-lain. Melalui pendefinisian ekstensi DICOM di *Supplement 30* (2001), standar meliputi juga data digital non-citra yang terkait dengan pasien seperti ECG dan *vital signs* lainnya berdasarkan rekaman data kurva. Ekstensi ini dikenal sebagai DICOM *waveform*. Tujuannya adalah untuk menjaga informasi yang direkam dalam format digital (non-citra), terbuka untuk pengukuran selanjutnya tanpa kehilangan kualitas [6]. Untuk penyimpanan di lokal, data medis ECG menggunakan standard SCP-ECG, sementara untuk pengiriman dan penyimpanan di server menggunakan standard DICOM *waveform*. Data medis dengan format DICOM ini akan disimpan di PACS (*Picture Archiving and Communication Systems*) server pusat.

Untuk operabilitas dan fleksibilitas yang baik digunakan kerangka kerja software berbasiskan teknologi web. Salah satu kerangka kerja yang terkenal dan banyak digunakan di dunia medis untuk tujuan pencatatan rekam medis elektronik adalah OpenEMR. Kerangka kerja ini menyertakan database menggunakan MySQL, web server, dan antar muka menggunakan web browser. OpenEMR juga telah menyertakan berbagai menu yang diperlukan dalam layanan medis. OpenEMR terpasang di sisi telemedicine cart dan sisi server pusat.

Untuk media komunikasi antar dokter menggunakan software komunikasi multimedia yang juga berbasis web. Software yang digunakan adalah jitsi untuk *video conferencing*, yaitu aplikasi gratis yang mendukung teknologi WebRTC. Aplikasi video conference ini mempunyai fitur yang bisa beradaptasi terhadap kondisi bandwidth jaringan yang tersedia dan bisa menjalankan hanya video, audio atau teks (*chatting*) saja.

Saat ini, telemedicine cart menggunakan sistem operasi Windows 10 dengan spesifikasi perangkat keras menggunakan Intel NUC7i7BNH dengan kemampuan prosesor Core i7 hingga 4 GHz. Sedangkan untuk server pusat, digunakan sistem operasi Linux dengan perangkat keras Fujitsu Primergy RX300 S7 dengan prosesor xeon E5 2 socket berkecepatan 2,30 GHz dan memori sebesar 16 GB. Saat ujicoba implementasi jitsi untuk *video conferencing* adalah dengan menempatkan jitsi video bridge (server) di *cloud* PMI-BPPT.

Sistem telemedicine BPPT memudahkan pengiriman data medis ECG dari dokter umum di puskesmas ke dokter spesialis di rumah sakit. Pengiriman data dilakukan melalui jalur komunikasi yang teramankan, misal menggunakan *secured copy* pada jalur publik atau disiapkan jaringan VPN (*Virtual Private Network*) tersendiri. Hasil diagnosis dari dokter spesialis bisa dengan cepat diterima oleh dokter umum untuk ditindaklanjuti. Demikian juga komunikasi untuk konsultasi antara dokter umum yang ada di puskesmas dengan dokter spesialis yang ada di rumah sakit dimudahkan melalui video conference.

Data rekam medis ECG dan dokumen hasil diagnosa yang dihasilkan dari sistem telemedicine ini termasuk kategori data yang sensitif dan rahasia sehingga perlu dijaga keamanannya. Keduanya data dalam format DICOM dan dokumen dalam format PDF ini dapat diverifikasi keabsahannya dengan modul penjamin keabsahan yang diimplementasikan pada sistem ini, yang konsepnya akan dijelaskan bersama dengan pembahasan tentang tanda tangan dan sertifikat digital.

Saat ini mekanisme penyimpanan dan penjaminan integritas rekam medis masih bersifat terpusat, dan menggunakan konsep *client-server* untuk pengelolaan dan pemanfaatannya. Teknologi lainnya yang belakangan ini aktif dibahas, dan dapat dimanfaatkan untuk menjamin integritas data medis adalah teknologi blockchain. Teknologi ini populer karena digunakan untuk mewujudkan beberapa mata uang *crypto*, seperti bitcoin, ethereum, dan sebagainya, yang aktif diperdagangkan dan dilakukan secara terdistribusi tanpa melalui otoritas kliring yang terpusat. Teknologi ini tergolong *peer-to-peer* dan didasarkan atas *distributed ledger* (blok catatan yang terdistribusi), di mana untuk tiap blok yang mencatat transaksi disertakan nilai *hash* yang memiliki ketergantungan dengan nilai-nilai *hash* dari blok-blok terdahuli pada mata rantai yang telah disepakati sebelumnya. Hal ini menjamin integritas data di setiap blok, karena pengubahan data atau rantai blok memerlukan penyesuaian nilai hash di blok-blok yang saling terkait. Untuk penggunaan pada penyimpanan rekam medis, di tiap blok bisa disertakan informasi terenkripsi terkait lokasi fisik rekam medis disimpan, dan pihak-pihak yang memiliki otentikasi dapat menggunakannya untuk mengambil data yang diperlukan [14]. Pemanfaatan teknologi blockchain juga mendukung pengelolaan akses dan perijinan pemanfaatan data, interoperabilitas dan pertukaran data antar pihak-pihak yang mengelola data rekam medis [1][7]. Selain itu, juga dilaporkan fleksibilitas dalam pengaksesan data medis tertentu yang dibuka untuk keperluan riset dan pengambil kebijakan, tanpa melanggar privasi pemilik data, untuk digunakan pada *big data analytics* [9].

Sistem telemedicine yang dikembangkan belum mengimplementasikan teknologi blockchain. Kajian dan pengembangan masih dilakukan secara terpisah, untuk memastikan kematangan teknologi dan kesiapan regulasi dalam pemanfaatannya. Sebagai contoh, dapat digunakan teknologi blockchain untuk konsolidasi data dari berbagai basis data lokal yang dikelola oleh penyedia jasa medis, dan dapat dimanfaatkan oleh pasien untuk berbagi data antarpenyedia jasa medis, perusahaan asuransi, pengambil kebijakan, dan lain-lain secara absah dan tanpa melanggar privasi.

III. TANDA TANGAN DIGITAL PADA RANAH MEDIS

Fleksibilitas yang ditawarkan oleh Internet dan teknologi informasi pada umumnya, harus juga dikaitkan dengan keamanan sistem yang seharusnya bersifat eksklusif, yaitu menjamin kerahasiaan, integritas, dan ketersediaan

informasi medis. Ada beberapa mekanisme keamanan informasi yang dapat dilakukan untuk menjamin ketiga faktor tersebut diantaranya adalah sebagai berikut [11]:

- Melakukan penilaian risiko untuk menentukan kerentanan sistem.
- Otentikasi dan tanda tangan digital sebagai kepastian integritas data.
- *Digital watermarking*.
- Implementasi dari komponen perangkat lunak keamanan data.
- Implementasi transmisi data yang aman menggunakan algoritma enkripsi yang berdasar pada PKI (*Public Key Infrastructure*).
- Implementasi arsitektur untuk mentransfer dan untuk mengakses data medis yang berada pada area *remote*.

Dari beberapa mekanisme di atas, pemanfaatan tanda tangan digital memastikan integritas data sehingga menjamin keabsahan data medis ECG dan dokumen analisa medis yang terkait. Integritas data, yang juga diikat dengan identitas pengguna, akan memperkuat kepercayaan (*trust*) dari para pelaku medis. Mekanisme tanda tangan digital yang memanfaatkan PKI (*Public Key Infrastructure*) ditunjukkan pada Fig. 2, yang mana melibatkan dua aktivitas utama, yaitu penandatanganan (*signing*) dan verifikasi (*verifying*). Dua aktivitas ini juga memanfaatkan *secure hash functions* yang memastikan dua dokumen berbeda akan memiliki nilai *hash* yang berbeda. Sebagai contoh, sebuah dokumen *M* ditanda tangan secara digital oleh pengguna *A*, maka dokumennya akan berisikan dokumen awal dan nilai *hash* yang telah dienkripsi dengan *private key* K_{pri} dari pengguna *A*, sebagai pernyataan keabsahan oleh pengguna *A*. Jika isi dokumen ini mengalami perubahan, maka akan mengalami kegagalan ketika diverifikasi sebagai berikut. Nilai *hash* dari dokumen original dapat didekripsi menggunakan *public key* K_{pub} dari pengguna *A*, dan dibandingkan dengan nilai *hash* yang dihitung dari dokumen yang hendak diuji keabsahannya.

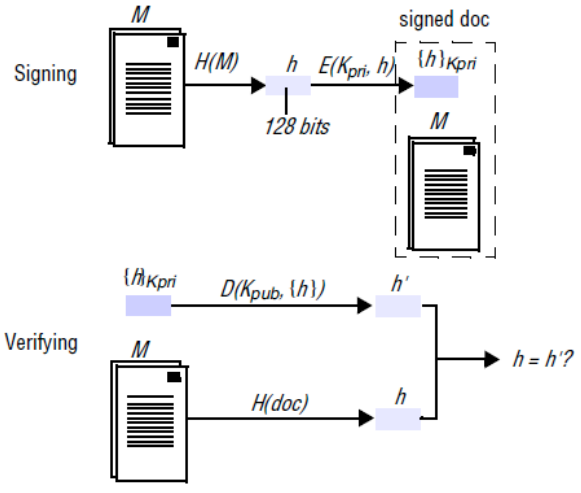

Fig. 2. Konsep Tanda Tangan Digital Menggunakan *Public Key* [4].

Untuk otentikasi penggunaan tanda tangan digital ini, dan untuk memperkuat kepercayaan pengguna, yaitu dokter spesialis, dokter umum, dan pasien, maka perlu disiapkan sertifikat digital yang diselaraskan dengan identitas dari dokter spesialis dan dokter umum di kehidupan nyata. Format sertifikat digital mengacu ke standar X.509 yang di dalamnya berisikan informasi nama pengguna, otoritas atau CA (*Certificate Authority*) yang mengeluarkan sertifikat, masa berlaku sertifikat, dan informasi administrasi lainnya. Di dalam sertifikat juga disertakan *public key* yang telah terikat dengan sertifikat ini, dan pengguna dapat memverifikasi keabsahan sertifikat pada rantai kepercayaan (*chains of trust*) dari otoritas yang mengeluarkan sertifikat ini.

Penerapan tanda tangan digital pada ranah medis tidak saja ditinjau dari aspek teknologi, tapi juga aspek legal, politis, kebijakan dan regulasi, dan penerimaan dari pelaku medis itu sendiri. Untuk kasus Indonesia, regulasi telemedicine yang idealnya juga menyertakan rekam medis elektronik masih sedang disusun oleh regulator, sehingga aktivitas kerekayasaan lebih ditekankan pada aspek teknologi, termasuk studi pustaka pengembangan dan uji coba yang dilakukan di negara-negara lain.

Regulasi di Indonesia yang menyertakan rekam medis di antaranya UU Nomor 29 tahun 2004 tentang Praktek Kedokteran dan Peraturan Menteri Kesehatan Nomor 269/Menkes/Per/2008 tentang Rekam Medis. Pada penjelasan pasal 46 ayat 3 dari UU Nomor 29 tahun 2004 disebutkan bahwa apabila pencatatan rekam medis menggunakan teknologi informasi elektronik, kewajiban membubuhi tanda tangan dapat diganti dengan menggunakan nomor identitas pribadi (*personal identification number*). Pasal 2 dari Peraturan Menteri Kesehatan di atas menyebutkan penyelenggaraan rekam medis dengan menggunakan teknologi informasi elektronik diatur lebih lanjut dengan peraturan tersendiri. Sedangkan pasal 5 ayat 5 menyebutkan bahwa dalam hal terjadi kesalahan dalam melakukan pencatatan pada rekam medis dapat dilakukan pembetulan, dan ayat 6 menyebutkan pembetulan sebagaimana dimaksud pada ayat 5 hanya dapat dilakukan dengan cara pencoretan tanpa menghilangkan catatan yang dibetulkan dan dibubuhi paraf dokter, dokter gigi, atau tenaga kesehatan tertentu yang bersangkutan. Hal-hal terkait rekam medis seperti disampaikan di atas sangat layak untuk diimplementasikan secara elektronik menggunakan tanda tangan dan sertifikat digital.

Peraturan yang relatif baru seperti Peraturan Menteri Kesehatan Nomor 46 tahun 2017 tentang Strategi E-Kesehatan Nasional telah menyertakan telemedicine dan rekam medis elektronik sebagai bagian dari strategi e-Health untuk mengatasi masalah infrastruktur, komunikasi, dan sumber daya manusia di sektor kesehatan. Namun, masih perlu ditunggu regulasi yang lebih konkrit untuk hal-hal yang disertakan pada strategi ini.

Jika hanya ditinjau dari ranah layanan TIK, penggunaan tanda tangan digital di Indonesia telah diperkuat oleh regulasi yaitu UU Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik dan PP Nomor 82 tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Selain itu, layanan komputasi awan juga harus berada di dalam koridor regulasi di atas, sehingga bisa disusun SLA (*Service Level Agreement*) antara penyedia layanan dan pemilik data medis dalam menjamin kerahasiaan dan kehandalan dari data medis yang tersimpan.

Tanda tangan digital menggunakan PKI telah digunakan oleh pelaku medis di Brazil [12], di mana para dokter memperoleh sertifikat digital yang terikat dengan identitas

mereka yang dikeluarkan oleh otoritas yang diakreditasi oleh *Brazilian Public Key Infrastructure* (ICP-Brasil). Seperti dijelaskan sebelumnya, sertifikat digital yang diterbitkan memiliki sepasang kunci kriptografi, yaitu *public key* dan *private key*. Untuk meningkatkan keamanan *private key* dapat disimpan pada hardware khusus seperti kartu cerdas atau *cryptographic token* menggunakan USB [5].

Negara lain yang juga menerapkan sistem telemedicine seperti yang dipaparkan pada makalah ini adalah Venezuela, di mana mekanisme pengamanan menggunakan sertifikat digital di Medical Center Teaching La Trinidad (CMDLT) dan daerah terpencil yang berlokasi di Municipalities Baruta dan Hatillo di Venezuela [11]. Penggunaan sertifikat digital dikelola dengan mekanisme yang memiliki ketetapan hukum yang kuat, dan tidak hanya digunakan untuk tanda tangan digital dalam menjamin keabsahan data, namun juga untuk penjaminan kerahasiaan dan integritas data dan dokumen analisa medis.

IV. Integrasi Modul Penjamin Keabsahan pada Sistem Telemedicine BPPT

Integrasi modul penjamin keabsahan data dan dokumen analisa medis pada sistem telemedicine BPPT dilakukan dengan menambahkan sertifikat digital pada data medis dengan format DICOM dan pada dokumen dengan format PDF. Pada Fig. 3 menunjukkan proses pengiriman data medis ECG dari ujung ke ujung (*end-to-end*). Bagian kotak berwarna merah adalah proses yang diperlukan untuk menyertakan modul penjaminan keabsahan data medis dan dokumen analisa medis. Modul ini diimplementasikan di sisi telemedicine cart (lokal) maupun di sisi server (pusat).

Di sisi lokal data ECG hasil akuisisi masih berupa raw data yang kemudian diubah ke dalam format SCP-ECG untuk disimpan di penyimpan lokal. Data ECG ini selanjutnya diubah lagi ke dalam format DICOM untuk dikirimkan ke server PACS. Proses penyertaan tandatangan digital dan sertifikat digital (*signing*) pada file DICOM dilakukan sebelum proses pengiriman. Tanda tangan dan sertifikat digital diselaraskan dengan identitas dokter umum di sisi lokal (puskesmas).

Di sisi server file DICOM yang sudah menyertakan tanda tangan digital akan diterima dan disimpan di server PACS. Proses verifikasi atau otentikasi terjadi ketika dokter spesialis di rumah sakit akan memeriksa data medis ECG dan membuat laporan hasil diagnosa (*report*). Apabila keabsahan data medis terverifikasi dokter spesialis bisa melanjutkan untuk membuat *report*.

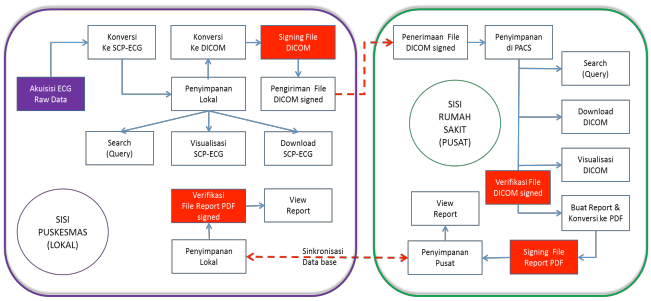

Fig. 3. Transmisi Data Medis ECG *end-to-end*.

Modul untuk penjaminan keabsahan data rekam medis ECG DICOM menggunakan dcmsign, yaitu bagian dari DCMTK sebuah kumpulan library dan aplikasi yang menerapkan sebagian besar standard DICOM dan banyak digunakan perusahaan di bidang medis untuk berbagai kebutuhan. Dcmsign membaca file DICOM dan menjalankan operasi penandatanganan digital. Terdapat dua operasi penandatanganan digital yang utama, yaitu: *signing* dan verifikasi (*verifying*) yang dijalankan melalui perintah dalam bentuk command line.

Selanjutnya di sisi server juga ada proses penjaminan keabsahan pada dokumen pelaporan hasil pemeriksaan dan diagnosa dari dokter spesialis. Dokumen laporan ini dibuat dalam format PDF. Pembuatan tanda tangan digital pada dokumen ini menggunakan PortableSigner. Program penandatanganan digital ini menggunakan sertifikat X.509 dan bersifat platform independen, berjalan di Linux, Windows dan Mac OS X.

Dokumen laporan yang telah bertandatangandigital disimpan di penyimpan pusat dan secara bersamaan data atributnya (yang salah satunya menunjukkan URL dari dokumen) juga disimpan di database OpenEMR pusat. Melalui proses sinkronisasi (replikasi) antara data base pusat dan lokal maka data atribut tersebut dapat diakses oleh dokter umum di puskesmas. Melalui data atribut URL dokumen dapat diunduh ke penyimpan lokal. Selanjutnya melalui modul verifikator dokter dapat melakukan otentikasi dokumen tersebut.

Proses pembuatan sertifikat digital belum terintegrasi dengan sistem telemedicine BPPT. Untuk tujuan pengujian dalam skala laboratorium, sertifikat digital belum dibuat melalui Certificate Authorities melainkan dibuat sendiri atau *self-signed*. Salah satu aplikasi yang dapat digunakan untuk menerbitkan sertifikat *self-signed* adalah GetaCert.

V. Uji Coba

Uji coba modul penjamin keabsahan data medis dilakukan dengan melakukan uji coba fungsional dan uji coba verifikasi dengan membandingkan file *hash* sebelum dan sesudah dilakukan modifikasi file yang telah diberikan tanda tangan digital. Hasil dari perbandingan ini kemudian akan ditampilkan pada modul verifikasi yang terintegrasi dengan sistem telemedicine.

Pada implementasi modul penjamin keabsahan data dan dokumen analisa medis, implementasi dilakukan dengan menggunakan *self-signed certificate* yang dibuat melalui aplikasi pembuat sertifikat digital. Penggunaan *self-signed certificate* dianggap memadai untuk uji coba skala laboratorium. Pada aplikasi pembuat sertifikat digital, dapat diisikan identitas pembuat *self-signed certificate* dengan mengisikan nama lengkap, identitas organisasi, dan alamat organisasi dari pembuat sertifikat. Fig. 4 memperlihatkan contoh *self-signed certificate* yang telah dibuat untuk kemudian digunakan membuat tanda tangan digital pada file hasil diagnosa dokter dan data medis ECG menggunakan format DICOM.

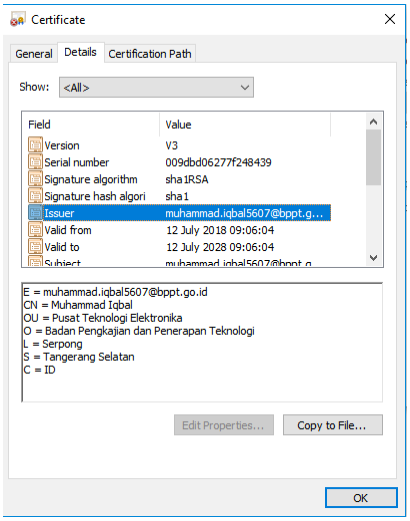

Fig. 4. *Self-Signed Certifcate* yang Digunakan.

Aplikasi yang digunakan dalam pembuatan tanda tangan digital untuk file PDF adalah PortableSigner. Tanda tangan digital yang diberikan ke file dokumen dapat ditambahkan atribut gambar berupa barcode maupun tanda tangan asli dokter spesialis. Fig. 5 memperlihatkan hasil tanda tangan digital pada file dokumen hasil diagnosa dokter. Dari hasil implementasi tersebut, terlihat tanda tangan digital masih berstatus *invalid* karena sertifikat digital yang digunakan tidak berasal dari CA (*Certificate Authority)*, sebuah badan atau lembaga yang memiliki kewenangan mengeluarkan sertifikat digital.

Fig. 5. Tanda Tangan Digital pada File Hasil Diagnosa Dokter.

Setelah dilakukan penambahan tanda tangan digital, dilakukan uji *hash* dengan menggunakan modul validator dan verifikator yang terintegrasi dengan sistem telemedicine. Hasil file yang telah diberikan tanda tangan digital, kemudian dilakukan perubahan untuk memverifikasi fungsional dari modul verifikator dan validator. Modul ini berfungsi untuk membandingkan antara file *hash* yang asli yang tersimpan di database dengan file *hash* yang telah diubah. Berikut tabel I memperlihatkan perbandingan file *hash* sebelum file diberikan tanda tangan digital, setelah file diberikan tanda tangan digital, dan setelah dilakukan perubahan pada file.

TABLE I. CONTOH PERBANDINGAN FILE *HASH* PADA DOKUMEN HASIL DIAGNOSA DOKTER.

Kategori	File Asli	File Tertanda Tangan Digital	File Setelah Dilakukan Perubahan
CRC32	2085ED1E	B3911BFE	368C1A5D
MD5	CA555FA6AB505 B1FB5EEFFAF76C 29DA5	F2E1F7935C54 216705E453CD41 9C7AD1	9D7FC03403 64936CBD68 22527A38DB94
SHA-1	DA7073A95B0F595 4EE8F73B13E464	91EA86D7D B9B3BADEF	5CB486C4E95 4277BB191C
	13CF8F372F9	22FCDE81C7C9 EB6A9 89488	3C5BCB929AEB 1B33DE4

Jika dilihat dari perbandingan ketiga file *hash* tersebut, terdapat perbedaan dari hasil verifikasi dan validasi dokumen. Sistem telemedicine akan menunjukkan kalau hasil verifikasi gagal. Kemudian, hasil dari verifikasi dan validasi akan ditampilkan pada perangkat sistem informasi telemedicine.

Implementasi tanda tangan digital pada file berformat DICOM dilakukan dengan menggunakan sertifikat digital *self-signed certificate* yang telah dibuat sebelumnya. Penambahan tanda tangan digital menggunakan aplikasi dcmsign. Aplikasi dcmsign menyokong algoritma MAC RIPEMD-160, SHA-1, MD5, SHA256, SHA384, dan SHA512. Pada pengujian, dilakukan implementasi SHA256 karena SHA256 umum digunakan dalam tanda tangan digital dan tidak banyak merubah jumlah besar kapasitas file. Uji coba dilakukan dengan membandingkan file *hash* sebelum dan sesudah dilakukan perubahan *tag attribute* pada file DICOM. File DICOM untuk ECG menggunakan format DICOM *waveform*, yang berisi data numerik aktifitas kelistrikan jantung dalam periode dan durasi tertentu. *Tag attribute* yang digunakan adalah nama pasien, nomor identitas pasien, usia, *timestamp*, jenis kelamin, DOB *(Date of Birth)*, dan instansi tempat bekerja. Fig. 6 memperlihatkan contoh tampilan ECG *chart* dari file ECG DICOM yang digunakan pada pengujian dengan identitas nama dari pasien adalah John Doe.

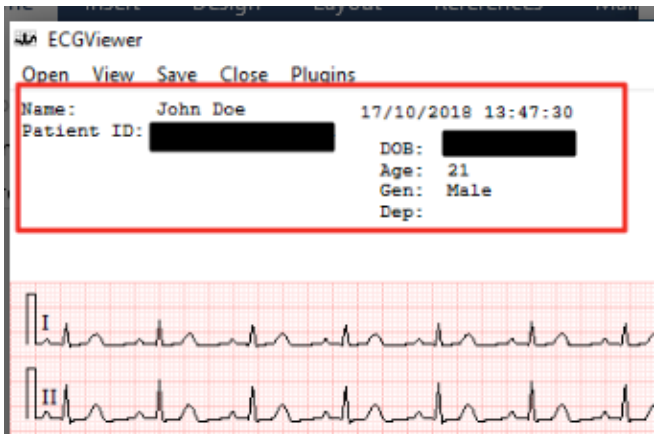

Fig. 6. Contoh Tampilan ECG *Chart* dari File DICOM *Waveform.*

Fig. 7 memperlihatkan hasil file DICOM yang telah diberikan tanda tangan digital beserta hasil verifikasi. Dari hasil verifikasi terdapat identitas tanda tangan digital berupa 1.2.276.0.7230010.3.1.4.1589530690.6944.15410614 22 dan status verifikasi OK. Kemudian dilakukan perubahan attribute nama pada file DICOM dengan merubah nilai attribute nama menjadi "Muhammad Iqbal". Tampilan ECG *chart* setelah perubahan ditunjukkan di Fig. 8. Perubahan ini mengubah struktur file sebelumnya menjadi struktur file baru dan membuat hasil verifikasi gagal. Hal ini ditunjukkan pada Fig. 9 di mana status hasil verifikasi gagal dan pesan notifikasi yang ditampilkan berupa *signature is invalid (document corrupted)*.

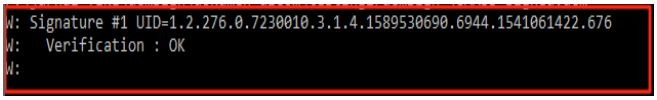

Fig. 7. Verifikasi Hasil Implementasi Tanda Tangan Digital pada *File* DICOM.

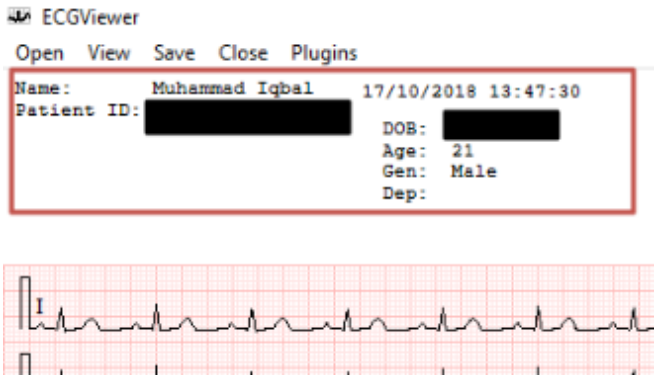

Fig. 8. Perubahan *Tag Attribute* Nama Pasien

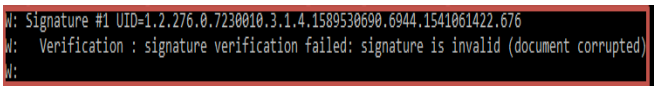

Fig. 9. Verifikasi File DICOM Setelah Dilakukan Perubahan *Tag Attribute* Nama Pasien.

Selain melalui modul verifikasi bawaan dari aplikasi, verifikasi dan validasi dilakukan juga melalui *hash* dari masing-masing file. Verifikasi ini dilakukan dengan membandingkan file *hash* sebelum dilakukan perubahan dan sesudah dilakukan perubahan. Hasil verifikasi dan validasi akan terlihat melalui sistem informasi telemedicine. Tabel II memperlihatkan perbandingan file *hash*, mulai dari file sebelum diberikan tanda tangan digital, setelah diberikan tanda tangan digital, dan file *hash* setelah dilakukan perubahan *tag attribute* nama pasien.

TABLE II. PERBANDINGAN FILE *HASH* PADA FILE DICOM

Kategori	**File Asli**	**File Tertanda Tangan Digital**	**File Setelah Dilakukan Perubahan *Tag Attribute***
CRC32	F7D185E1	36B3E6E5	73C56246
MD5	00D1DC96A3ED3 33 15CE5E76EE7BF 3 883	C52FE0F7204BBA E446E4A32B8EC 07EDD	BA5B24DEEA 9F8298F0963E 3E619EC686
SHA-1	026A649F9150327 ABDB0F3964324 C 5D636 3010EC	A47EAAC3B16A 5E57DC2523B48 5AC07F653909 E89	5CE4CC5B8A 94E0D883330 D25608731694 F 3F7D49

Jika dilihat dari perbandingan ketiga file *hash* tersebut, terdapat perbedaan dari ketiganya. Perbedaan file *hash* sebelum dan sesudah dilakukan perubahan *tag attribute* nama pasien, mengindikasikan bahwa terjadi perubahan data dan keabsahan data medis tidak bisa diverifikasi. Hasil ini memberikan kesimpulan bahwa file telah berubah dan keabsahan data DICOM tidak bisa dipertanggungjawabkan.

VI. PENUTUP

Makalah ini telah memaparkan penambahan modul keabsahan data pada sistem telemedicine yang dikembangkan oleh PTE-BPPT. Hasil-hasil uji coba menunjukkan data medis ECG dalam format DICOM dan analisa medis dalam format PDF dijamin integritasnya setelah diikat dengan tanda tangan digital. Perubahan data oleh pihak-pihak yang tidak berwenang terdeteksi saat dilakukan verifikasi, dan dapat ditunjukkan oleh fasilitas sistem informasi yang disediakan.

Pekerjaan selanjutnya adalah menyempurnakan sistem telemedicine dengan menyertakan sertifikat digital dari otoritas yang terakreditasi, misal iOTENTIK yang dikeluarkan oleh BJIK-BPPT. Setelah itu, diperlukan uji coba keabsahan data pada situasi riil di lokasi layanan kesehatan.

VII. BIBLIOGRAPHY

[1] A. Azaria, A. Ekblaw, T. Viera and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," in *Proc. 2nd International Conference on Open and Big Data*, 2016.

[2] BPPT, Program Manual 2015-2019 Tahun Anggaran 2018: Inovasi Konvergensi Teknologi Elektronika dan Telekomunikasi Sistem Elektromedika (Inovasi Teknologi Telemedicine), Jakarta, 2018.

[3] K. Buse and S. Hawkes, "Health in the sustainable development goals: ready for a paradigm shift?," *Globalization and Health,* vol. 11, no. 13, 2015.

[4] J. Coulouris, J. Dollimore, T. Kindberg, G. Blair, *Distributed Systems: Concepts and Design*, Addison-Wesley, 2012.

[5] A. Espitia, K. Ortega, E. Romero and I. Jaramillo, "Authentication and Digital Signature USB Device for Telemedicine Applications," in *7th International Caribbean Conference on Devices, Circuits and Systems*, 2008.

[6] R. Fensli, "Evaluation of international standards for ECG-recording and storage for use in tele-medical services," Agder University College, Grimstad, 2006.

[7] J. D. Halamka, A. Lippman and A. Ekblaw, "The Potential for Blockchain to Transform Electronic Health Records," *Harvard Business Review,* 2017.

[8] S. Kovacevic, M. Kovac and J. Knezovic, "System for Secure Data Exchange in Telemedicine," in *9th International Conference on Telecommunications - ConTel 2007*, Zagreb, 2007.

[9] P. T. S. Liu, "Medical Record System Using Blockchain, Big Data and Tokenization," in *Proc. International Conference on Information and Communications Security (ICICS)*, 2016.

[10] I. Sachpazidis, Image and Medical Data Communication Protocols for Telemedicine and Teleradiology, PhD Dissertation, TU Darmstadt, 2008.

[11] T. Vivas, A. Zambrano and M. Huerta, "Mechanisms of Security Based on Digital Certificates Applied in a Telemedicine Network," in *30th Annual International IEEE EMBS Conference*, Vancouver, 2008.

[12] A. Von Wangenheim, R. F. Custódio, J. E. Martina, I. d. B. Giuliano and R. l Andrade, "User Satisfaction with Asynchronous Telemedicine a Study of Users of Santa Carina's System of Telemedicine and Tele-Health," *REV ASSOC MED BRAS,* vol. 59, no. 3, pp. 209-212, 2013.

[13] M. E. Whitman and H. J. Mattord, Management of Information Security, Cengage, 2014.

[14] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa and X. Zhang, "BBDS Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments," *Information,* vol. 8, no. 44, 2017.