Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) DOI: 10.25126/jtiik.201961471
Vol. 6, No. 5, Oktober 2019, hlm. 475-484 p-ISSN: 2355-7699
Akreditasi KEMENRISTEKDIKTI, No. 30/E/KPT/2018 e-ISSN: 2528-6579

PENERAPAN TANDA TANGAN DIGITAL PADA GAMBAR FORMULIR C1.PLANO-KWK DI PILKADA SULAWESI SELATAN

Rachmawan Atmaji Perdana[1], Dhika Rizki Anbiya[2], Andrari Grahitandaru[3]

[1,3]Pusat Teknologi Informasi dan Komunikasi – Badan Pengkajian dan Penerapan Teknologi
[2]Balai Jaringan Informasi dan Komunikasi – Badan Pengkajian dan Penerapan Teknologi
Email: [1]rachmawan.atmaji@bppt.go.id, [2]dhika.rizki@bppt.go.id, [3]andrari.grahitandaru@bppt.go.id

(Naskah masuk: 20 Desember 2018, diterima untuk diterbitkan: 02 Oktober 2019)

Abstrak

Sengketa pemilihan umum presiden 2014 telah mendatangkan ribuan kotak suara ke Jakarta sebagai bukti hukum. Gambar-gambar form C1 yang merupakan salinan rekapitulasi hasil di TPS yang sudah diunggah di situs web KPU, ternyata tidak dapat dijadikan sebagai bukti hukum karena tidak bisa dibuktikan keabsahannya sebagai dokumen elektronik. Tanda tangan digital merupakan bukti otentik yang terdapat pada dokumen elektronik. Penggunaan tanda tangan digital dapat memastikan keutuhan dan keaslian suatu dokumen elektronik sehingga dapat dipertanggungjawabkan secara hukum. Hal ini menjadi salah satu alasan dilakukannya penerapan tanda tangan digital pada formulir model C1.PLANO-KWK. Formulir ini merupakan berita acara hasil pemungutan dan penghitungan suara pemilihan umum di tempat pemungutan suara. Formulir tersebut diambil gambarnya menggunakan aplikasi berbasis ponsel Android untuk kemudian ditandatangani secara digital. Hasil gambar yang telah ditandatangani selanjutnya ditampilkan pada situs web penayangan. Hal ini diterapkan pada Pemilihan Umum Daerah Sulawesi Selatan atas kerja sama antara Badan Pengkajian dan Penerapan Teknologi, Komisi Pemilihan Umum Provinsi (KPU), dan KPU Daerah Kota Makassar pada tanggal 27 Juni 2018. Makalah ini membahas mengenai teknologi yang digunakan untuk melakukan tanda tangan digital. Pada implementasinya hanya sebesar 0,32% dari seluruh TPS yang menerapkan tanda tangan digital dan sebesar 7,61% sertifikat digunakan dari total sertifikat yang telah diterbitkan.

Kata kunci: *tanda tangan digital, pemilu, pilkada, keamanan informasi, penyelenggara sertifikasi elektronik*

DIGITAL SIGNATURE IMPLEMENTATION ON C1.PLANO-KWK FORM SCREENSHOT IN SOUTH SULAWESI LOCAL ELECTION

Abstract

The dispute over the 2014 presidential election brought thousands of ballot boxes to Jakarta as legal evidence. C1 form image, which is a copy of the recapitulation of results at the TPS, have been uploaded on the KPU website, apparently cannot be legal evidence because it cannot be proven the validity of the electronic document of the C1 form. Digital signature is an authentic proof embedded in an electronic document. It shows the integrity, authenticity, and non-repudiation of a document, so it can be used as a legal evidence. This become one of the reason of the implementation of digital signature in C1.PLANO-KWK form. C1.PLANO-KWK form is an evidence proof of voting recapitulation process in voting place. Android application capture the image of this form, and digitally signed it. This image is then showed on the display website. This has been implemented in South Sulawesi Regional Election on June 27 2018 by cooperation between Agency of Assessment and Application of Technology (BPPT) and Election Commission (KPU) of South Sulawesi Province and City of Makassar. This paper only describes about the technologies which are used in digital signing process. Only 0.32% of the voting place has implementing digital signature in its C1.PLANO-KWK form, and only 7.61% of the digital certificate that has been published used to digitally signed the C1.PLANO-KWK form.

Keywords: *digital signature, election, local election, information security, certification authority*

1. PENDAHULUAN

Sidang sengketa Pemilu Presiden 2014 merupakan proses sengketa yang sangat mahal dimana kotak suara dari berbagai daerah dibawa ke Mahkamah Konstitusi Jakarta sebagai bukti hukum dimana hakim ingin melihat hasil perolehan di tiap TPS dalam form plano. Form C1 yang merupakan salinan form plano TPS sudah diunggah di situs web KPU, seharusnya dapat menjadi bukti hukum,

sehingga tidak perlu mendatangkan ribuan kotak suara dari berbagai daerah di Indonesia. Namun ternyata Form C1 yang diunggah tersebut tidak dapat dijadikan bukti hukum karena tidak dapat dibuktikan keabsahan dokumen elektroniknya terutama siapa yang mengirim dan bertanggungjawab terhadap konten form C1 yang sudah diunggah tersebut.

Tanda tangan digital adalah salah satu perkembangan utama dalam dunia keamanan jaringan dan data. Kebutuhan akan tanda tangan digital meningkat seiring dengan pertumbuhan komunikasi digital. Algoritme tanda tangan digital mengautentikasi integritas dari data yang ditandatangani dan identitas dari penandatangan. Autentikasi pada tanda tangan digital adalah proses dimana penerima dari pesan digital dapat mempercayai integritas pesan dan pengirimnya.

Tanda tangan digital telah diimplementasikan dalam berbagai proses bisnis, terutama terkait pemerintahan. Di Amerika Serikat, Percetakan Pemerintah menerbitkan versi elektronik dari hukum umum dan privat, anggaran negara, dan keputusan kongres. Universitas Chicago, Stanford, dan Penn. State juga telah menerbitkan transkrip nilai mahasiswa yang dibubuhi tanda tangan digital (Barik & Karforma, 2012). Di Malaysia, tanda tangan digital juga digunakan untuk memvalidasi transaksi perbankan (Saripan & Hamin, 2011). Dalam makalah ini tanda tangan digital digunakan pada Form C1.PLANO-KWK yang merupakan form hasil penghitungan suara perolehan suara setiap calon. Form ini difoto langsung dari ponsel Android dan aplikasi mengirim langsung dari TPS oleh petugas yang bertanggung jawab terhadap proses penghitungan suara tersebut. Sebelum proses pengiriman tentunya petugas tersebut sudah meregistrasikan sertifikat digital untuk dirinya menggunakan NIK dan surel yang menyatakan bukti diri dan identitas petugas tersebut. Dalam beberapa detik dokumen elektronik tersebut ditayangkan dalam situs web dan kelak dapat dijadikan bukti hukum ketika terjadi sengketa pemilu di Mahkamah Konstitusi tanpa harus mendatangkan kotak suara ke Mahkamah konstitusi sebagai bukti hukum.

Tanda tangan digital merupakan pengganti tanda tangan basah pada dokumen elektronik. Penggunaan tanda tangan digital pada dokumen elektronik tertuang dalam UU 19 tahun 2016 tentang perubahan UU no. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik serta turunannya PP no. 82 tahun 2012 tentang Penyelenggara Sistem dan Transaksi Elektronik, suatu dokumen Elektronik yang dibubuhi Tanda Tangan Elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi persyaratan yang ditentukan dan dapat disamakan dengan akta otentik. Tanda tangan tersebut merupakan sebuah berkas berupa sertifikat yang diamankan menggunakan kata sandi dengan enkripsi tertentu yang digunakan untuk menunjukkan identifikasi seseorang atau pihak tertentu secara online. Sertifikat digital diterbitkan oleh *Certification Authority* dimana Kementerian Komunikasi dan Informatika bertindak sebagai *root* CA. Saat ini terdapat dua lembaga Penyelenggara Sertifikasi Elektronik (PSrE) yang terdaftar untuk pemerintah yaitu Badan Pengkajian dan Penerapan Teknologi (BPPT) dan Badan Siber dan Sandi Negara (BSSN).

Tanda tangan digital pada makalah ini menggunakan sertifikat yang diterbitkan oleh BPPT yang memiliki nama iOTENTIK. Penerbitan sertifikat diberikan untuk setiap Tempat Pemungutan Suara (TPS) atas nama salah satu petugas KPPS di seluruh provinsi Sulawesi Selatan. Sertifikat tersebut kemudian digunakan untuk melakukan tanda tangan pada gambar hasil pengambilan gambar/citra melalui kamera ponsel pintar dengan aplikasi Android yang telah dibuat sebelumnya. Hasil gambar yang telah ditandatangani berupa gambar yang telah dibubuhi tanda air dan kemudian ditampilkan pada situs web beserta tanda tangan digital berekstensi p7s. Tanda tangan digital ini berisi informasi penandatangan dan hirarki penerbitan sertifikat, sehingga dapat dipertanggungjawabkan keabsahan dan keasliannya.

2. KERANGKA TEORI

Pada bagian ini akan dijelaskan beberapa kerangka teori yang digunakan pada makalah, diantaranya adalah sertifikat digital, kriptografi kunci publik, format *keystore* PKCS#12, tanda tangan digital, *Cryptographical Message Syntax* (CMS) dan *message queue*.

2.1 Kriptografi Kunci Publik

Kriptografi kunci publik, atau kriptografi asimetrik, adalah skema enkripsi dan dekripsi yang menggunakan dua kunci yang secara matematis berelasi, namun tidak identik, yakni kunci publik dan kunci privat. Dua pekerjaan utama yang menggunakan kriptografi kunci publik adalah tanda tangan digital (yang akan dijelaskan lebih lanjut dalam makalah ini), dimana konten ditandatangani secara digital dengan kunci privat individual dan diverifikasi oleh kunci publik individu yang bersangkutan. Pekerjaan yang lain adalah enkripsi, dimana konten dienkripsi oleh kunci publik individual dan hanya dapat dienkripsi oleh kunci privat individu yang bersangkutan (GlobalSign Corporation, t.thn.).

2.2 Sertifikat Digital

Sertifikat digital adalah kredensial/mandat digital yang memberikan informasi tentang identitas dari suatu entitas, beserta informasi-informasi lainnya. Sertifikat digital dapat diibaratkan sebagai surat izin mengemudi, kartu tanda penduduk, surat nikah, atau bentuk-bentuk identitas lainnya. Perbedaannya adalah bahwa sertifikat digital berhubungan dengan sistem infrastruktur kunci

publik. *Certification Authority* (CA) adalah organisasi atau perusahaan yang menerbitkan sertifikat digital. CA memiliki tanggung jawab besar untuk memastikan keabsahan sertifikat yang diterbitkan. CA harus memastikan bahwa sertifikat yang diterbitkannya diberikan ke pihak yang benar.

Komponen-komponen dasar dalam sertifikat digital adalah :

- Nama dari pengguna/entitas yang memiliki sertifikat
- Kunci publik dari pengguna/entitas
- Nama dari CA
- Tanda tangan digital sertifikat tersebut

Sertifikat digital yang diterbitkan oleh CA iOTENTIK berformat X.509 versi 3. Standar X.509 versi 3 mendefinisikan empat belas ekstensi sebagai usaha untuk mengkonsolidasi ekstensi-ekstensi yang paling banyak digunakan oleh pihak ketiga. Dari keempat belas ekstensi standar yang didefinisikan oleh X.509v3, hanya ada empat yang digunakan secara luas, yakni ekstensi `basicConstraints`, `keyUsage`, `extKeyUsage`, dan `crlDistributionPoints` (Chandra, et al., 2002).

Sertifikat digital berformat X.509 memiliki beberapa field yaitu *Version, Serial Number, Signature, Issuer, Validity, Subject, Subject Public Key Info, Unique Identifiers*, dan *Extensions*. *Field Subject* mengidentifikasi entitas yang berasosiasi dengan kunci publik yang tersimpan dalam *field* kunci publik subyek. Field ini harus mengandung *Distinguished Name* (DN) X.500. DN ini harus unik untuk masing-masing entitas subyek yang disertifikasi oleh satu CA yang didefinisikan oleh *field* `issuer` (Cooper, et al., 2008).

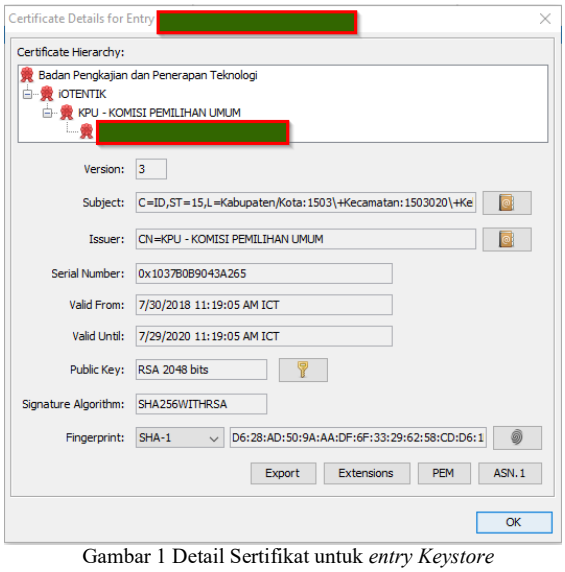
2.3 Format *Keystore* PKCS# 12

Sertifikat digital berformat X.509, jika berdiri sendiri, belum memiliki kunci privat, yang akan digunakan untuk melakukan penandatanganan digital. Sertifikat digital, kunci privat, dan kunci-kunci simetrik yang terkait dengannya akan disimpan dalam suatu format berkas yang disebut *keystore* (O'Brien & Weir, 2008). iOTENTIK menggunakan format *keystore* PKCS#12. Konten-konten dalam keystore PKCS#12 dilindungi dengan *passphrase* (kata kunci). *Entry* dalam berkas PKCS#12 yang didistribusikan oleh iOTENTIK adalah bertipe *key entry*.

Gambar 1 mengilustrasikan detail sertifikat pada salah satu *entry keystore* yang diterbitkan oleh iOTENTIK.

2.4 Tanda Tangan Digital

Tanda tangan digital adalah teknik matematika yang digunakan untuk memvalidasi otentisitas dan integritas dari suatu pesan, perangkat lunak, maupun dokumen digital. Tanda tangan digital bekerja berdasarkan kriptografi kunci publik.



Gambar 1 Detail Sertifikat untuk *entry Keystore*

Berikut adalah proses penandatangan dokumen secara digital secara matematis (diasumsikan m adalah dokumen/pesan yang akan ditandatangani, a adalah kunci publik, dan x adalah kunci privat (Smech, 2001) :

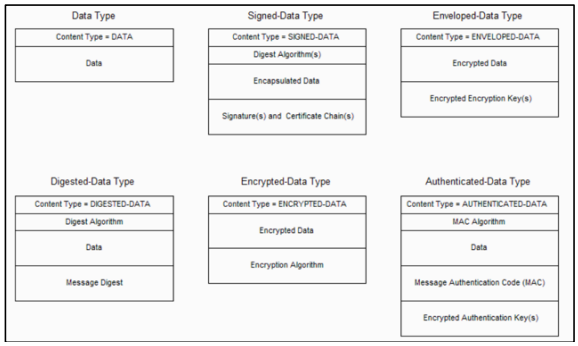
1. Menghitung *hash* (*message digest*) dari dokumen/pesan yang akan ditandatangani dengan suatu fungsi *hashing* h, yang didefinisikan sebagai $p = h(m)$. Dimana p adalah *hash* dari m.
2. Melakukan penandatanganan terhadap p dengan menggunakan fungsi *signing*/enkripsi u dan kunci privat x, untuk menghasilkan tanda tangan digital s. Persamaan matematikanya adalah $s = u(p, x)$. Alasan mengenkripsi nilai *hash* dari dokumen bukannya mengenkripsi seluruh dokumen adalah fungsi *hash* dapat mengkonversi sembarang masukan menjadi suatu nilai yang panjangnya tetap, yang biasanya lebih pendek dari dokumen asli.
3. s, m, dan a dikirim dari penandatangan ke pengguna yang akan menerima pesan.
4. Penerima pesan akan memverifikasi tanda tangan dengan cara menggunakan fungsi dekripsi v, yang akan mengevaluasi persamaan $p' = v(a, s)$. Selain itu penerima juga akan menghitung *message digest* dari dokumen/pesan tersebut dengan persamaan $p = h(m)$. Jika $p = p'$ maka tanda tangan digital pada dokumen tersebut adalah valid.

Tanda tangan digital digunakan untuk menjamin keaslian pengirim atau penerima dokumen elektronik, menjamin keutuhan dokumen (tidak ada perubahan terhadap dokumen), serta nir-sangkal bagi pemilik sebuah dokumen elektronik (Mehmood, 2018).

2.5 Cryptographical Message Syntax

Cryptographic Message Syntax (CMS) adalah sintaks yang digunakan untuk menandatangani, men-*digest*, mengotentikasi, atau mengenkripsi sembarang

konten pesan digital. Spesifikasi CMS umumnya cukup untuk mendukung berbagai tipe konten. CMS mendefinisikan satu konten proteksi, `ContentInfo`. `ContentInfo` mengenkapsulasi tipe konten teridentifikasi tunggal, dan tipe identifikasi dapat menyediakan enkapsulasi yang lebih jauh. CMS mendefinisikan enam tipe konten : *data*, *signed-data*, *enveloped-data*, *encrypted-data*, dan *authenticated-data*.



Gambar 2. Jenis *Cryptographical Message Syntax Format*

Implementasi yang sesuai dengan spesifikasi CMS harus mengimplementasi konten proteksi, `ContentInfo`, dan harus mengimplementasi tipe konten data, *signed-data*, dan *enveloped-data*, Tipe konten lainnya mungkin juga diimplementasikan. CMS juga dikenal dengan nama lamanya, format *Public Key Cryptography Standard* (PKCS) #7 (Housley, 2009).

Konten *signed-data* berisi dari konten dari sembarang tipe dan nol atau lebih nilai *signature*. Sembarang jumlah penandatangan secara paralel dapat menandatangani sembarang tipe dari konten. Proses dimana *signed-data* dibuat melibatkan langkah-langkah sebagai berikut :

1. Untuk masing-masing penandatangan, *message digest*, atau nilai *hash*, dihitung pada konten dengan algoritma *message digest* spesifik untuk penanda tangan tersebut. Jika penandatangan menandatangani informasi selain dari konten, message digest dari konten dan informasi lainnya di-*digest* dengan algoritma *message digest* penandatangan, dan hasilnya disebut dengan "*message digest*".
2. Untuk masing-masing penandatangan, *message digest* ditandatangani secara digital menggunakan kunci privat penandatangan.
3. Untuk masing-masing penandatangan, nilai *signature* dan informasi penandatangan tertentu dikumpulkan ke dalam nilai `SignerInfo`. Sertifikat-sertifikat dan CRL-CRL untuk masing-masing penandatangan, dan yang tidak berkorespondensi dengan penandatangan manapun, dikumpulkan di langkah ini.
4. Algoritma *message digest* untuk semua penandatangan dan nilai `SignerInfo` untuk semua penandatangan dikumpulkan bersama-sama dengan dengan content ke dalam nilai `SignedData`.

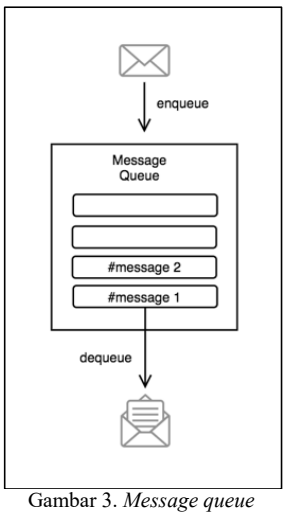
Penerima pesan secara terpisah menghitung *message digest*. *Message digest* ini dan kunci publik penandatangan digunakan untuk memverifikasi nilai *signature*. Kunci publik penandatangan direferensikan baik dengan *distinguished name* pengirim bersama-sama dengan *serial number* spesifik dari pengguna atau dengan *subject key identifier* yang secara unik mengidentifikasi sertifikat yang mengandung kunci publik. Sertifikat penandatangan dapat disertakan pada field sertifikat di `SignedData` (Housley, 2009).

2.6 Message Queue

Message adalah data yang diangkut di antara aplikasi pengirim dan penerima; pada dasarnya merupakan *byte array* dengan beberapa *header* diatasnya. Contoh dari pesan dapat berupa sesuatu yang memberitahu sebuah sistem untuk memulai memproses suatu tugas, ia dapat mengandung informasi mengenai tugas yang selesai atau hanya berupa pesan saja.

Queue (antrian) adalah baris dari sesuatu yang menunggu untuk ditangani – dalam rangkaian berurutan dimulai dari awal baris. Message queue adalah antrian dari pesan-pesan (message) yang dikirimkan antar aplikasi. Ini termasuk rangkaian dari objek-objek kerja yang menunggu untuk diproses.

Arsitektur dasar dari *message queue* adalah sederhana, ada sebuah aplikasi klien yang dinamakan produser yang membuat pesan dan mengirimkannya ke *message queue*. Aplikasi lainnya, dinamakan *consumer*, menyambung ke *queue* dan mengambil pesan untuk diproses. *Message-message* ditempatkan ke dalam *queue* dan disimpan hingga *consumer* mengambilnya (Johansson, 2014).



Gambar 3. *Message queue*

3. RANCANG BANGUN SISTEM

Sistem ini terdiri dari dua bagian, yakni klien dan server. Data citra dan tanda tangan digital formulir C1.PLANO-KWK diambil oleh aplikasi

Android di sisi klien, yang kemudian dikirimkan ke server penerima. Setelah pesan diterima, kemudian akan diverifikasi oleh server. Jika verifikasi berhasil, citra form C1.PLANO-KWK akan ditampilkan di web penayangan yang dapat diakses oleh publik.

Metode perancangan sistem yang digunakan adalah *Rapid Application Development* (RAD). Metode ini dipilih karena memiliki keunggulan dalam segi waktu pengembangan sistem (Sasmito & Wiyono, 2017). Tahapan-tahapan pada metode RAD adalah perencanaan kebutuhan, desain dan implementasi.

3.1 Perencanaan Kebutuhan

Pada tahapan ini dilakukan beberapa pertemuan dengan Komisi Pemilihan Umum (KPU) Provinsi Sulawesi Selatan dan iOTENTIK BPPT. KPU merupakan pihak penyelenggara pemilihan umum dan iOTENTIK BPPT sebagai penerbit sertifikat digital yang akan digunakan pada aplikasi.

Pertemuan dengan KPU dilakukan untuk melihat proses bisnis yang berjalan semetara pertemuan dengan iOTENTIK dilakukan untuk kebutuhan integrasi dan teknis penerbitan sertifikat. Hasil dari beberapa pertemuan yang telah dilakukan dirumuskan bahwa sistem yang akan dibangun membutuhkan tiga elemen penting yaitu aplikasi klien dan aplikasi server. Dokumen yang akan ditandatangani berupa hasil foto formulir C1.PLANO-KWK yang kemudian akan dikirimkan ke server untuk ditayangkan hasilnya pada situs penayangan.

3.2 Desain

Tahapan ini merupakan tindak lanjut dari tahapan perencanaan kebutuhan yaitu desain untuk aplikasi klien dan aplikasi server. Perancangan aplikasi klien menggunakan aplikasi mobile Android. Sementara itu aplikasi server meliputi implementasi server MQTT dan situs web penayangan menggunakan *framework* PHP Code Igniter.

3.3 Implementasi

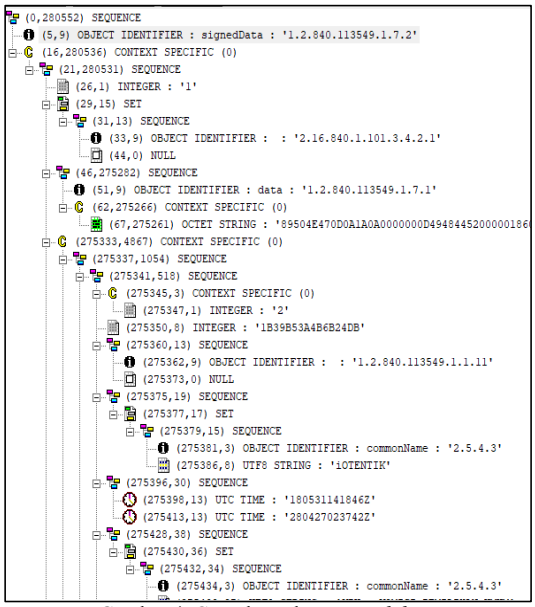
Tahap selanjutnya merupakan implementasi dari hasil desain. Implementasi meliputi aplikasi klien, aplikasi server dan penyimpanan sertifikat digital pada aplikasi Android.

3.3.1 Aplikasi Klien

Aplikasi di sisi klien berbasis Android dan ditulis dalam bahasa pemrograman Java. Ada tiga fitur yang diimplementasikan di aplikasi ini, yaitu pengambilan citra form C1.PLANO-KWK menggunakan kamera ponsel, pembuatan tanda tangan digital citra form C1.PLANO-KWK dalam format CMS, serta pengiriman berkas tanda tangan digital berformat CMS tersebut melalui protokol *message queue*.

Pembuatan berkas berformat CMS dari penandatanganan citra form C1.PLANO-KWK diimplementasikan dengan bantuan pustaka Bouncy Castle (bouncycastle.org, t.thn.). Pustaka Bouncy Castle telah menyediakan sebuah kelas umum untuk membuat pesan pkcs7-signature, yaitu kelas `CMSSignedDataGenerator`. Sertifikat digital yang digunakan untuk menandatangani berkas citra tersebut adalah sertifikat digital yang telah diinstal di ponsel Android, yang dipilih lewat menu antarmuka pengguna.

Kelas `CMSSignedDataGenerator` menerima masukan dari object `ContentSigner`, yang merupakan antarmuka umum yang mampu untuk membuat tanda tangan digital dari stream keluaran. Namun, `ContentSigner` hanya mampu menghasilkan tanda tangan digital jika diberikan masukan berupa data pesan dan kunci privat. Sedangkan, dalam API KeyStore Android, data kunci privat tidak dapat diambil ke memori. Oleh karena itu, dibutuhkan pustaka lain yang dapat membantu untuk menghasilkan data tanda tangan digital berformat CMS, jika diberikan input berupa data pesan dan hasil enkripsi dari hash data pesan tersebut dengan menggunakan kunci privat. Pustaka tambahan yang digunakan adalah j4sign, yang merupakan ekstensi dari pustaka Bouncy Castle (Servizio Sistema Informativo, t.thn.).



Gambar 4. Contoh struktur *signed data*

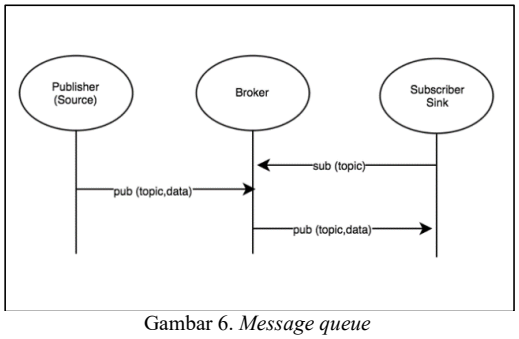
Data berformat CMS yang dihasilkan sesuai dengan format yang ditentukan oleh standar IETF RFC-5652. Data yang dihasilkan bertipe *signed data* yang memiliki struktur yang dituliskan dalam *syntax* ASN.1 sebagai berikut :

```
SignedData ::= SEQUENCE {
        version CMSVersion,
        digestAlgorithms
DigestAlgorithmIdentifiers,
        encapContentInfo
EncapsulatedContentInfo,
        certificates [0] IMPLICIT
CertificateSet OPTIONAL,
        crls [1] IMPLICIT
RevocationInfoChoices OPTIONAL,
        signerInfos SignerInfos }

      DigestAlgorithmIdentifiers ::= SET
OF DigestAlgorithmIdentifier

      SignerInfos ::= SET OF SignerInfo
```

Gambar 5. Standar struktur *signed data* dalam *syntax* ASN.1 berdasarkan IETF-RFC 5652

Berkas CMS yang dihasilkan memiliki tipe *attached signature* yang berarti data asal juga dilampirkan dalam berkas CMS, selain tanda tangan digital dari data tersebut (oracle.com, 2018). Pada struktur *signed data*, data asal diletakkan dalam *field encapContentInfo*.

Pengiriman data tanda tangan digital ke server dilakukan dengan menggunakan protokol *message queue*. Untuk mengimplementasi proses ini di perangkat *smartphone* Android, digunakan pustaka MQTT. MQTT adalah singkatan dari *Message Queuing Telemetry Transport*. MQTT sangat ideal untuk perangkat yang terhubung dan aplikasi mobile di era M2M/IoT dimana *bandwidth* dan daya baterai menjadi pertimbangan utama.



Gambar 6. *Message queue*

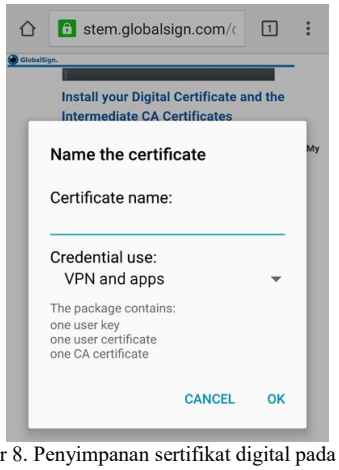
Protokol MQTT menggunakan prinsip *publish-subscribe*. Komponen yang menghasilkan info tertentu dan menerbitkan info tersebut disebut *publisher*. Di sini aplikasi di ponsel Android bertindak sebagai *publisher*. Klien yang tertarik untuk mendapatkan info tertentu mendaftar diri minat dari info tertentu, proses ini disebut *subscribe*, klien yang berminat disebut *subscriber*. *Subscriber* di sini adalah aplikasi di server penerimaan. Selain *publisher* dan *subscriber* ada juga *broker* yang menjamin *subscriber* mendapatkan info yang diinginkan dari *publisher*. Aplikasi klien akan mengirimkan data ke suatu *topic* di *broker* yang telah ditentukan sebelumnya.

Berikut adalah tampilan antarmuka aplikasi klien. Gambar kamera besar di bagian tengah layar berfungsi untuk mengambil gambar. Tombol "Pilih Alias" berfungsi untuk memilih kredensial yang akan menandatangani citra. Tombol "Digital Signing + Kirim Data" berfungsi untuk menandatangani berkas citra dan menyimpannya dalam format CMS, serta mengirimkannya ke server.

Gambar 7. Tampilan antar muka aplikasi Android

3.3.2 Penyimpanan Sertifikat Digital pada Aplikasi

Untuk melakukan instalasi sertifikat digital dalam *storage* kredensial ponsel Android, terlebih dahulu harus memiliki berkas sertifikat digital berformat PKCS#12 yang diterbitkan oleh iOTENTIK. Sertifikat tersebut harus diekstrak dan saat ekstraksi akan dilakukan, pengguna harus memasukkan *passphrase* yang sesuai untuk sertifikat digital tersebut. Kemudian, pengguna harus memberikan nama untuk sertifikat digital tersebut (Hallberg, 2016).



Gambar 8. Penyimpanan sertifikat digital pada *device*

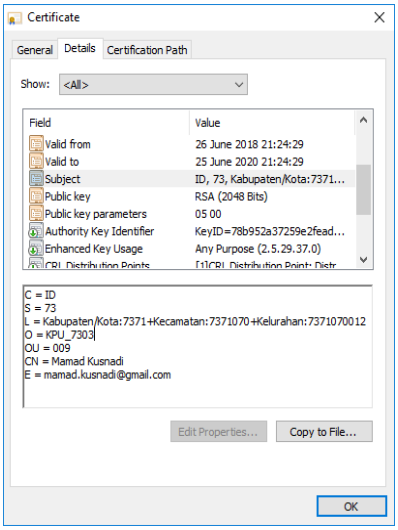
Di sisi aplikasi, untuk mengakses kunci privat dan rantai sertifikat yang berpasangan dengannya dalam *storage* kredensialnya, dapat dilakukan dengan menggunakan kelas `KeyChain` yang telah disediakan oleh API pemrograman Android. Aplikasi yang mengakses `KeyChain` biasanya melalui langkah-langkah berikut ini (Android Developer, 2018) :

1. Menerima panggilan balik dari `X509KeyManager` bahwa ada permintaan untuk mengambil kunci privat.
2. Memanggil method `choosePrivateKeyAlias` untuk mengizinkan pengguna untuk memilih dari daftar kunci privat dan rantai sertifikat yang berpasangan dengannya. Alias terpilih akan dikembalikan oleh callback `KeyChainAliasCallback.alias(String)`, atau null jika tidak ada kunci privat yang tersedia atau pengguna membatalkan permintaan.
3. Memanggil `getPrivateKey(Context, String)` dan `getCertificateChain(Context, String)` untuk mengambil kredensial untuk kembali ke panggilan balik `X509KeyManager` pasangannya.

3.3.3 Aplikasi Server

Sistem penerimaan pesan di server terdiri atas *broker* MQTT dan aplikasi subscriber dari topic di *broker* MQTT yang telah ditentukan sebelumnya. Aplikasi subscriber akan melakukan verifikasi terhadap data yang diterima, serta meletakkan konten data yang ada di dalam berkas CMS ke folder yang sesuai untuk ditampilkan di situs web.

Sama halnya dengan aplikasi klien yang menggunakan pustaka Bouncy Castle untuk membuat berkas tanda tangan digital berformat CMS, aplikasi *subscriber* di server juga akan menggunakan pustaka Bouncy Castle untuk melakukan verifikasi terhadap data yang diterima di *broker* MQTT.



Gambar 9. Informasi *Distinguished Name* (DN)

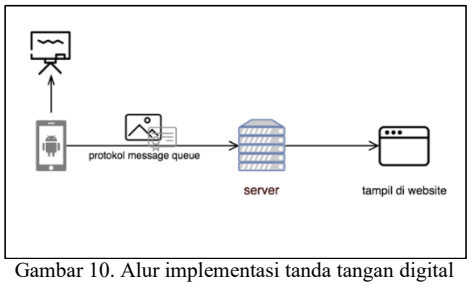
Informasi penandatangan diperoleh dari *field* DN (*Distinguished Name*) yang ada di sertifikat penandatangan yang disertakan dalam berkas CMS. Informasi-informasi ini digunakan untuk menentukan di folder mana data konten (berkas citra C1.PLANO-KWK) akan diletakkan. Informasi-informasi yang ada di *field* DN meliputi :

1. Alamat *Email* (E) pemilik
2. *Common Name* (CN) yaitu nama pemilik sertifikat digital
3. *Organization Unit* (OU), yaitu nomor TPS
4. *Organization* (O), yaitu kode KPU provinsi
5. *Locality* (L), meliputi kode kabupaten/kota, kode kecamatan, dan kode kelurahan
6. *State* (ST) yaitu kode provinsi
7. *Country* (C), yaitu kode negara

4. HASIL DAN PEMBAHASAN

Pada bagian ini akan dijabarkan dalam dua bagian yaitu implementasi dan verifikasi keabsahan gambar.

4.1 Implementasi

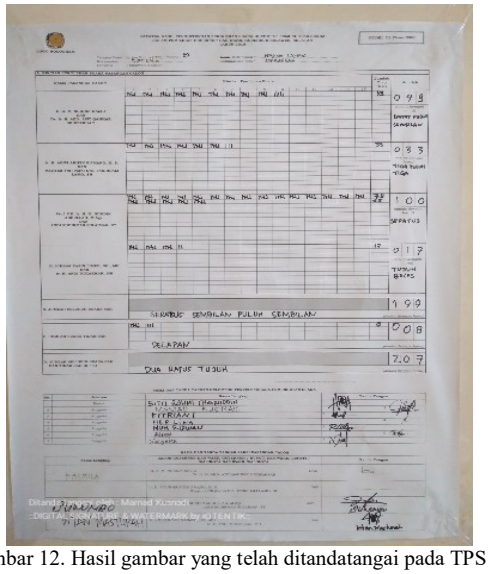


Gambar 10. Alur implementasi tanda tangan digital

Alur implementasi dimulai dari petugas TPS yang memiliki sertifikat digital melakukan pengambilan citra formulir C1.PLANO-KWK melalui aplikasi Android. Setelah itu gambar yang telah diambil secara otomatis ditandatangani oleh aplikasi dan diberi tanda air berisi informasi nama pengirim gambar dan informasi instansi penerbit sertifikat digital.

Gambar 11. Situs web penayangan informasi formulir C1.PLANO-KWK yang telah ditandatangani

Gambar yang telah ditandatangani kemudian dikirim ke *server* melalui protokol *message queue* untuk selanjutnya ditampilkan pada situs web. Informasi yang ditampilkan pada situs web adalah tempat pengambilan gambar meliputi kota/kabupaten, kecamatan, kelurahan TPS beserta gambar yang telah diberi tanda air dan sertifikatnya. Penelusuran gambar yang telah berhasil ditandatangani dan terkirim ke situs web dilakukan dengan cara memilih kota/kabupaten beserta kecamatan dan kelurahan.



Gambar 12. Hasil gambar yang telah ditandatangai pada TPS 06 Kelurahan Pisang Utara

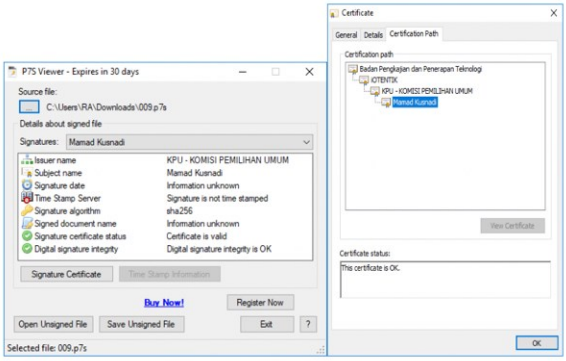
Sistem ini diimplementasikan pada Pemilihan Kepala Daerah Langsung Tingkat I Sulawesi Selatan tanggal 27 Juni 2018. Pada kenyataanya, implementasi menghadapi beberapa kendala diantaranya adalah koneksi internet yang tidak stabil sehingga koneksi ke server terputus. Total sertifikat yang telah diterbitkan oleh iOTENTIK sejumlah 709 namun sertifikat yang secara aktif digunakan hanya sebanyak 54 sertifikat pada 17.140 TPS yang ada di provinsi Sulawesi Selatan dengan detail pada tabel berikut.

Tabel 1 Jumlah gambar yang telah ditandatangani pada tiap kabupaten/kota di Propinsi Sulawesi Selatan

No	Kabupaten/Kota	Jumlah Gambar
1	Kabupaten Bantaeng	9
2	Kabupaten Bone	2
3	Kabupaten Jeneponto	2
4	Kabupaten Luwu Utara	4
5	Kabupaten Takalar	2
6	Kota Makassar	38
7	Kota Palopo	1
8	Kota Pare-Pare	1
	Jumlah	59

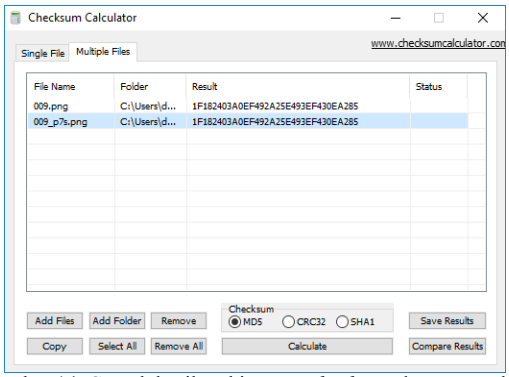
4.2 Verifikasi Keabsahan Gambar

Sertifikat yang dihasilkan dari proses penandatanganan gambar adalah berupa berkas berbentuk p7s. Saat ini masih dibutuhkan aplikasi untuk membaca isi dari sertifikat tersebut yaitu dengan menggunakan aplikasi P7S Viewer yang dapat diunduh dan bersifat *trial* selama 30 hari. Jika data yang tersimpan dalam berkas p7s otentik, maka P7S Viewer akan menampilkan pesan "*Digital signature integrity is OK*", artinya bahwa nilai dekripsi dari *hash* terenkripsi data awal dengan menggunakan kunci publik penandatangan sama dengan nilai *hash* dari data awal. Informasi yang dapat dilihat diantaranya adalah mengenai informasi penandatangan berupa DN dan hirarki penerbitan sertifikat.



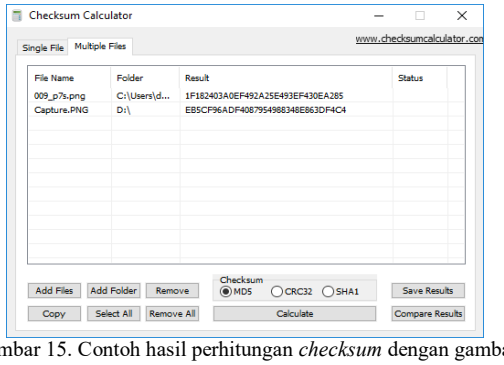
Gambar 13. Informasi mengenai detail sertifikat digital (gambar kiri merupakan informasi umum, sebelah kanan merupakan hirarki badan penerbit sertifikat)

Verifikasi keabsahan gambar yang ditampilkan di situs web dilakukan dengan melihat hasil perhitungan *checksum* dari gambar yang dimuat pada berkas berekstensi p7s dengan gambar yang disertakan pada situs web. Perhitungan *checksum* dapat dilakukan menggunakan aplikasi Checksum Calculator maupun kalkulator *checksum* yang tesedia secara daring di internet.



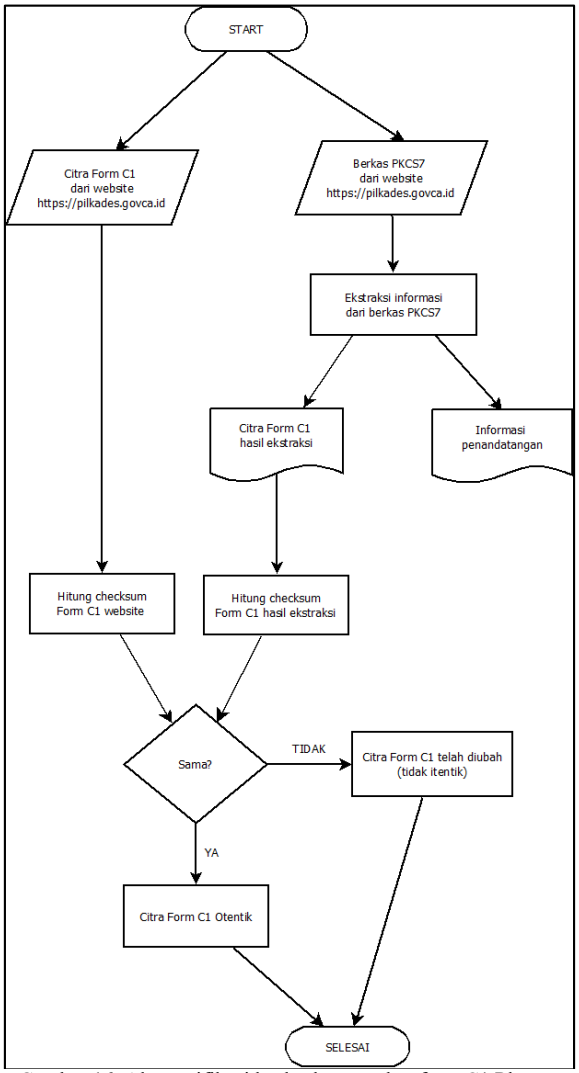
Gambar 14. Contoh hasil perhitungan *checksum* dengan gambar yang otentik

Apabila hasil perhitungan kedua gambar memiliki nilai yang sama, artinya gambar tersebut adalah otentik. Sebaliknya, apabila hasil perhitungan *checksum* tidak memiliki nilai yang sama, maka gambar yang ditampilkan di situs web tersebut dapat dipastikan telah dimodifikasi.



Gambar 15. Contoh hasil perhitungan *checksum* dengan gambar yang telah dimodifikasi

Untuk lebih jelasnya mengenai alur verifikasi keabsahan gambar form C1.Plano bertanda tangan digital dapat dilihat pada Gambar 16.



Gambar 16. Alur verifikasi keabsahan gambar form C1.Plano-KWK yang diunggah ke situs web https://pilkades.govca.id

5. KESIMPULAN DAN SARAN

Implementasi tanda tangan digital pada gambar C1.PLANO-KWK secara umum berjalan sesuai tujuan, namun mengalami beberapa kendala baik kendala teknis maupun non teknis. Kendala teknis dapat ditanggulangi. Protokol *message queue* membantu proses pengiriman gambar ke server yang dilakukan secara serentak setelah penghitungan suara karena dapat memastikan bahwa gambar benar-benar terkirim. Adapun nilai implementasi tanda tangan digital di TPS masih sangat rendah yaitu sebesar 0,32% dari seluruh TPS. Selain itu pula nilai penggunaan sertifikat digital juga masih sangat rendah yaitu sebesar 7,61%. Inilah kendala non teknis yang dihadapi karena uji coba pengiriman ini sifatnya sukarela, dan bukan tugas wajib KPPS.

Implementasi sertifikat digital pada makalah ini dilakukan pada gambar, untuk selanjutnya dapat dikembangkan dengan menggunakan protokol pengiriman lain maupun dengan menggunakan tipe berkas lain seperti pdf.

DAFTAR PUSTAKA

ANDROID DEVELOPER, 2018. *KeyChain.* [online] Tersedia di: <https://developer.android.com/reference/android/security/KeyChain> [Diakses 10 Juli 2018].

BARIK, N. & KARFORMA, S., 2012. A Study on Efficient Digital Signature Scheme for E-Governance Security. *Global Journal of Computer Science and Technology,* 12(3).

BOUNCYCASTLE.ORG, t.thn. *CMSSignedDataGenerator (Bouncy Castle Library 1.60 API Specification).* [online] Tersedia di: <https://www.bouncycastle.org/docs/pkixdocs1.5on/org/bouncycastle/cms/CMSSignedDataGenerator.html> [Diakses 10 Mei 2018].

CHANDRA, P., MESSIER, M. & VIEGA, J., 2002. *Network Security with OpenSSL.* Sebastopol: O'Reilly Media.

COOPER, D. et al., 2008. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.* [online] Tersedia di: <https://www.rfc-editor.org/info/rfc5280>

GLOBALSIGN CORPORATION, t.thn. *What is Public-key Cryptography?.* [online] Tersedia di: <https://www.globalsign.com/en/ssl-information-center/what-is-public-key-cryptography/> [Diakses 28 September 2018].

HALLBERG, L., 2016. *How to Download and Install a PKCS#12 onto Your Android Device.* [online] Tersedia di: <https://www.globalsign.com/en/blog/installing-certificates-onto-android-devices/>

HOUSLEY, R., 2009. *Cryptographic Message Syntax (CMS).* [online] Tersedia di: <https://www.rfc-editor.org/info/rfc5652>

JOHANSSON, L., 2014. *What is message queueing.* [online] Tersedia di: <https://www.cloudamqp.com/blog/2014-12-03-what-is-message-queuing.html> [Diakses 5 Februari 2018].

MEHMOOD, A., 2018. *Introduction to Digital Signatures and PKCS #7.* [online] Tersedia di: <https://www.cryptomathic.com/news-events/blog/introduction-to-digital-signatures-and-pkcs-7>

O'BRIEN, M. & WEIR, G. R., 2008. *Understanding Digital Certificates. Proceedings of the 2nd International Conference on Cybercrime Forensics Education & Training*.

ORACLE.COM, 2018. *Attached and Detached Digital Signatures.* [online] Tersedia di: <https://docs.oracle.com/cd/E19398-01/820-1228/gfnmj/index.html> [Diakses 13 Juli 2018].

SARIPAN, H. & HAMIN, Z., 2011. The Application of the Digital Signature Law in Securing Internet Banking: Some Preliminary Evidence from Malaysia. *Procedia Computer Science,* Volume 3, pp. 248-253.

SASMITO, G. W. & WIYONO, S., 2017. Implementation of Rapid Application Development Method on Academic Staff System of Harapan Bersama Polytechnic. *International Journal of Computer Trends and Technology (IJCTT),* 50(1).

SERVIZION SISTEMA INFORMATIVO, t.thn. *j4sign.* [online] Tersedia di: <http://j4sign.sourceforge.net/> [Diakses 5 Juni 2018].

SMECH, K., 2001. *Cryptography and Public Key Infrastructure on the Internet.* Hoboken: John Wiley & Sons Inc..