Altenatif Pembentukan Token Listrik di Sistem Listrik Prabayar Menggunakan Enkripsi AES

Khoirunnisa Afifah (13512077)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13512077@std.stei.itb.ac.id

***Abstrak*— Listrik prabayar menggunakan token untuk transfer pertambahan kuota listrik. Pembuatan dan pendistribusian token ini ditetapkan standarnya menggunakan Standard Transfer Specification (STS) oleh Eskom di Afrika Selatan. Pembentukan token melibatkan pembangkitan *decoder key* dan algoritma enkripsi terhadap format token yang disepakati. Makalah ini akan mencoba menggunakan AES yang merupakan algoritma standar enkripsi kunci simetris sebagai algoritma alternatif untuk pembentukan token listrik prabayar.**

***Kata Kunci*—listrik prabayar, Token, STS, AES.**

I. PENDAHULUAN

Sistem listrik prabayar mulai digunakan pada tahun 1993 di Afrika Selatan dan diterapkan di Indonesia sejak 2007. Layanan ini banyak diminati karena pelanggan dapat mengontrol penggunaan listrik mereka tiap bulannya. Kini Indonesia tercatat sebagai negara dengan jumlah pengguna listrik prabayar tebesar di dunia.

Pada sistem listrik prabayar, setiap pengguna memiliki meter prabayar khusus dengan nomor unik untuk setiap meter yang dapat menghitung sisa kuota listrik yang dimiliki pelanggan. Ketika jumlah kuota habis, pelanggan dapat menambah kuota listrik dengan cara membeli pulsa listrik ke PLN, Bank, ataupun gerai-gerai yang bekerjasama dengan PLN. Pelanggan diminta untuk memberikan nomor meteran dan jumlah kWh yang akan dibeli. Kemudian pelanggan akan mendapatkan 20 digit token, token inilah dimasukkan ke meteran listrik prabayar dan kemudian diurai menjadi penambahan kuota listrik.

Sampai saat ini sistem listrik prabayar menggunakan standard yang sama di seluruh dunia yaitu STS (*Standard Spesification Transfer*) yang dikelola oleh ESKOM. STS mendefinisikan informasi apa saja yang harus ada pada pembentukan token, kemudian token diubah menjadi 20 digit angka menggunakan algoritma yang ada pada STA (*Standard Transfer Algoritm*).

Makalah ini bertujuan untuk memberikan alternatif lain untuk pembentukan token, namun masih mengikuti standar yang ada pada STS.

II. DASAR TEORI

A. Meter STS

Seperti yang sudah dijelaskan sebelumnya, meter listrik prabayar yang ada saat ini mengikuti standar yang disebut *Standard Transfer Specification*. Tujuannya adalah agar penyedia layanan listrik tidak perlu membuat sistem yang berbeda-beda untuk setiap meter yang dibeli dari produsen yang berbeda.

Mekanisme kerja meter STS secara umum adalah sebagai berikut :

1. Setelah diproduksi meter akan dicoba menggunakan *factory code*.
2. PLN yang menerima meter dari pabrik akan mengubah *factory code* tersebut menjadi kode awal dari PLN.
3. Saat dipasang di pelanggan, PLN akan memasukkan kode aktivasi.
4. Setelah kode aktivasi dimasukkan akan di generate *decoder key* yang digunakan untuk *encoding* dan *decoding* token.

Pada setiap pembelian kuota listrik, PLN akan mengambil *decoder key* sesuai nomor meteran dan menggunakannya bersama dengan jumlah kWh dan waktu pembelian untuk membentuk 20 digit token yang dapat diubah oleh meter listrik menjadi jumlah kuota listrik yang harus ditambah.

B. Standar token menurut STS

STS mendfinisikan beberapa standar untuk token. Standar pertama adalah fungsi token. Fungsi token dapat merupakan *dispenser spesific* yaitu hanya mendukung transfer token dari pengelola token, di Indonesia PLN, kepada klien/kelompok klien (meter listrik) tertentu, fungsi ini memerlukan enkripsi pada token. Selain itu fungsi token dapat juga berupa *non-dispenser spesific* dimana token dibuat untuk dapat digunakan oleh semua klien.

Standar kedua adalah format token. Panjang token harus 66 bit. Dua bit digunakan sebagai kelas token dan empat bit sebagai subkelas token. Kelas dan subkelas token ini menentukan kegunaan dari token, misalnya

kelas 0 dan subkelas 0 digunakan untuk transfer kuota listrik, kelas 1 subkelas 0 untuk aktivasi, kelas 2 dan subkelas 0 digunakan untuk mengatur maksimum daya, dll. Empat bit digunakan untuk nomor random agar kemungkinan adanya token yang sama semakin kecil. Selain itu 24 bit digunakan untuk *timestamp* berupa jumlah menit sejak 1 Januari 1993. Kemudian 16 bit mendefinisikan jumlah kuota listrik yang dibeli dan 16 bit untuk CRC *checksum.*

Standar berikutnya adalah mekanisme transfer dan *encoding* token. Cara pertama yaitu menggunakan *magnetic card* yang hanya dapat digunakan sekali. Cara kedua adalah menggunakan *Numeric Token Technology*. Metode ini mengubah token menjadi string angka berukuran 20 digit. Cara transfer dari pengelola token ke klien hanya memerlukan kertas tanda bukti pembelian atau bahkan dapat diingat oleh pengguna. Cara inilah yang digunakan oleh PLN.

Standar tersebut menjamin bahwa token yang dihasilkan hanya dapat diterima oleh meter yang dituju, hanya dapat dibuat oleh pihak yang berwenang, hanya dapat digunakan sekali,dan tidak bisa dimodifikasi selama transfer antara pengelola listrik dan pengguna.

C. AES

AES adalah salah satu algoritma blok cipher yang digunakan sebagai standar enkripsi kunci simetris sampai saat ini. AES bekerja dengan ukuran blok 128-bit dan panjang kunci yang bervariasi antara 128, 192, 256 bit. AES bekerja dalam beberapa putaran bergantung pada panjang kunci. AES-128 bekerja dengan sembilan putaran, AES-192 sebelas putaran dan AES-256 dengan 13 putaran.

Sebelum melakukan putaran, AES membangkitkan semua kunci internal untuk tiap putaran. Pembangkitan dilakukan dengan menerapkan permutasi, difusi dan operasi XOR, yang dimulai dari kunci eksternal kemudian terhadap kunci pada putaran sebelumnya.

Pada AES plaintext dan kunci diletakkan pada persegi 4x4. Di setiap putarannya AES menerapkan *confussion* menggunakan s-box, difusi menggunakan permutasi baris, dan penggabungan bit-bit kolom. Di akhir setiap putarannya hasil perhitungan tadi di xor dengan kunci internal.

Setelah dilakukan putaran sesuai dengan panjang kunci, dilakukan putaran final. Putaran terakhir ini dilakukan sama seperti putaran sebelum-sebelumnya hanya saja tidak ada proses penggabungan bit-bit kolom.

III. HASIL DAN PEMBAHASAN

A. Rancangan proses pembuatan token

Dalam makalah ini digunakan algoritma AES untuk melakukan enkripsi terhadap data pada token. AES dipilih karena terjamin keamanannya. Selain itu AES dapat diimplementasikan dengan efisien pada hardware, mengingat kemampuan komputasi mikrokontroller pada meter listrik pasti terbatas.

Karena AES bekerja dalam panjang blok 128 bit, harus dilakukan beberapa perubahan terhadap format token yang diterapkan selama ini. Format token yang baru adalah sebagai berikut :

1. Panjang token 130 bit, dengan 2 bit pada token digunakan untuk kelas token dan tidak dienkripsi.
2. Subkelas token tetap menggunakan 4 bit.
3. *Timestamp* yang lama (24 bit) maksimum dapat digunakan hanya sampai 24 November 2024. Pada format baru ini panjang *timestamp* berubah menjadi 26 bit, sehingga dapat digunakan sampai tahun 2123. *Timestamp* digunakan untuk memastikan bahwa token belum pernah digunakan dan tidak kadaluwarsa.
4. Jumlah kuota listrik yang dibeli tetap 16 bit yang dibagi menjadi dua bagian, pangkat dalam basis 10 menggunakan dua bit dan mantissa 14 bit.
5. Jumlah bit untuk random number bertambah menjadi 14 bit.
6. Terdapat nomor meter pada format token yang baru. Nomor meter dicantumkan untuk memastikan bahwa token tersebut ditujukan kepada meter yang benar. Apabila setelah dienkripsi nomor meter yang didapat berbeda maka token tidak akan diproses. No meter biasanya 11 digit dengan dua digit untuk kode manufaktur, delapan digit kode serial meter, dan satu digit untuk perhitungan Formula Luhn. No meter menggunakan bit sejumlah 36.
7. CRC yang digunakan berubah dari CRC-16 menjadi CRC-32.

Token yang akan dibahas pada makalah ini adalah token jenis *dispenser specific*, dimana bit-bit token dienkripsi kecuali 2 bit kelas token. Bit kelas token akan disisipkan di akhir setelah token selesai dienkripsi. Penyisipan dua bit token tersebut dilakukan dengan cara meletakkan dua bit token kelas pada posisi bit ke 65 dan 66 (dengan LSB di posisi 0, dan MSB di posisi 127).

B. Pembentukan *decoder key*

Pembentukan *decoder key* yang digunakan pada makalah ini sesuai dengan algortima DKGA02 yang ada pada [3] dengan perubahan agar sesuai untuk AES. Algoritma ini memerlukan 16-digit Control Blok, 16-digit Pan Blok, serta kunci acak berukuran 128 bit.

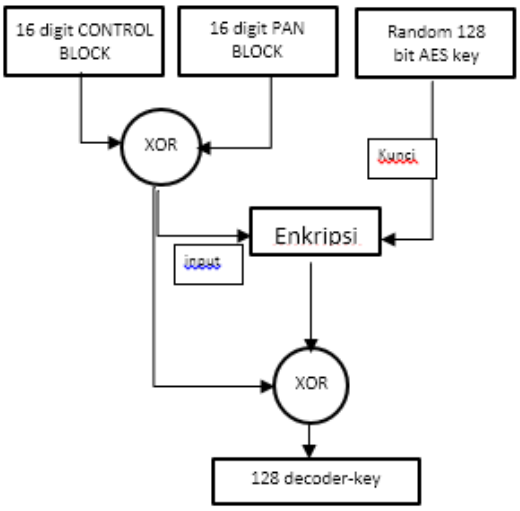
Control Blok merupakan sekumpulan hexadesimal yang terdiri dari dua digit tipe kunci, 6 digit kode grup pemasok, dua digit tarif indeks, satu digit angka revisi kunci, serta enam digit padding value.

Sedangkan Pan blok adalah sekumpulan angka dalam hexadesimal yang mengidentifikasikan meter listrik. Blok ini berisi 6 digit nomer identifikasi penerbit serta 11 digit nomor meter.

Nilai random 128 bit ini merupakan nilai initial yang akan dimasukkan oeh petugas PLN pada setiap meter

baru. Nilainya akan sama dengan nilai yang dicatat pada basis data PLN.

Secara garis besar algoritma pembentukan key yang digunakan dijelaskan oleh diagram berikut :



Gambar 1 Diagram pembentukan kunci

Perlu diketahui bahwa *decoder key* ini tidak tetap nilainya. *Decoder key* akan di bentuk ulang apabila ada perubahan terhadap tarif indeks, nomor revisi kunci, kode grup pemasok, tipe kunci, dan nomor kadaluwarsa kunci. Untuk pembentukan *decoder key* berikutnya kunci random yang akan digunakan adalah *decoder key* yang lama. Sehingga dapat dipastikan bahwa perubahan pada basis data di PLN akan sama dengan perubahan pada meter listrik pelanggan, meskipun tidak ada komunikasi antar keduanya

Decoder key yang telah terbentuk selanjutnya akan digunakan oleh pemasok listrik (PLN) sebagai kunci untuk membuat token dan digunakan oleh setiap meter listrik untuk menguraikan token yang diperoleh dari PLN untuk mendapatkan data-data token yang diperlukan.

C. Contoh proses pembuatan token

Percobaan pembuatan token dilakukan dengan menggunakan library javax.crypto yang ada di pada bahasa Java

- Perhitungan *decoder key*
  Misalkan nomor meter seseorang 06 2282 2746 6 dan IIN 600097 didapatkan PAN Bloknya 0009706228227466.
  Sedangkan control blok yang digunakan adalah 1 990400 03 1 FFFFFF
  Nilai XOR antara PANBlok dengan ControlBlok yaitu 3E1480306593F1F7 menjadi data input untuk AES
  Nilai acak 128-bit : 3961057639662976 menjadi kunci enkripsi *decoder key*
  Hasil enkripsi dalam byte array menghasilkan -39 83 33 0 -73 79 -37 -42 -89 -123 71 80 105 63 74 113
  Kemudian didapat decoder key nya : -22 22 16 52 -113 127 -24 -26 -111 -80 126 99 47 14 12 70

- Pembentukan token
  Token format yang akan digunakan :
  Kelas – 00 (Transfer Credit)
  Subkelas – 0000 (Listrik)
  Timestamp untuk 10 Mei 2015 pukul 09:00
  Total : 11.756.700 menit
  Dalam biner : 00101100110110010010011100
  Jumlah kuota listrik yang dibeli : 1638,3 kWh
  Dalam biner : 0011111111111111
  Random number : 11011001010100
  Nomer meter : 06 2282 2746 6
  00010111001100111011001101011000101 0
  CRC-32 terhadap semua data diatas
  11000100010011100001101000011011

  Didapat nilai token sebelum dienkripsi :
  00 00000010 11001101 10010010 01110000 11111111 11111111 01100101 01000001 01110011 00111011 00110101 10001010 11000100 01001110 00011010 00011011

  Kemudian dilakukan enkripsi menggunakan *decoder key* : -22 22 16 52 -113 127 -24 -26 -111 -80 126 99 47 14 12 70 (dalam array byte)
  Menghasilkan nilai :
  -89 -22 99 111 10 -100 -114 127 -78 -69 -77 -91 -101 124 -84 126 (dalam byte array)
  Maka token yang dihasilkan adalah :
  10110000 00101011 00111001 00100001
  11101010 11000110 11100011 00000000
  10011010 10001000 10011000 10110100
  11001001 00000110 10100111 00000101
  Disisipi bit class yang tidak ikut di enkripsi menjadi :
  10110000 00101011 00111001 00100001
  11101010 11000110 11100011 00000000 00
  10011010 10001000 10011000 10110100
  11001001 00000110 10100111 00000101

D. Pembahasan

Dari hasil analisis terhadap proses pembuatan token dan pembuatan *decoder key*, dapat dilihat bahwa token yang dibuat masih memenuhi batasan integritas STS dimana token hanya dapat diterima oleh meter yang dituju, hanya dapat dibuat oleh pihak yang berwenang, hanya dapat digunakan sekali,dan tidak bisa dimodifikasi selama transfer antara pengelola listrik dan pengguna.

Batasan pertama yaitu hanya dapat diterima oleh meter yang dituju dipenuhi karena setiap meter memiliki decoder key yang unik yang dibentuk salah satunya menggunakan nomor meter. Selain itu token juga dibentuk menggunkan nomor meter untuk pengecekan ulang. Apabila setelah token diuraikan didapatkan nomor meter yang berbeda dengan nomor yang dicatat, token akan ditolak.

Batasan pertama hanya dapat dibuat oleh pihak yang berwenang dipenuhi karena *decoder key* hanya diketahui oleh pihak yang mengeluarkan meter di awal dan melakukan perubahan terhadap tarif indeks, nomor revisi kunci, kode grup pemasok, tipe kunci, dan nomor kadaluwarsa kunci.

Batasan ketiga hanya dapat digunakan sekali terpenuhi dengan adanya *timestamp* dalam setiap token. Meter listrik menyimpan 50 token terakhir yang digunakan pada saat transaksi. Apabila *timestamp* pada token yang dimasukkan sudah ada di daftar token atau telah lewat dari waktu saat ini, berdasar hasil perhitungan oleh meter listrik maka token akan ditolak.

Batasan terakhir yaitu tidak bisa dimodifikasi selama transfer dipenuhi oleh CRC-32 yang ditambahkan di akhir token. Apabila ada perubahan pada token maka hasil perhitungan CRC tidak akan cocok, dan token ditolak.

Meskipun memenuhi syarat integritas STS, token yang dihasilkan apabila diubah menjadi nilai desimal akan menghasilkan 40 digit token. Nilai ini dua kali panjang token sebelumnya. Seharusnya dapat dicari cara dimana panjang digit token akhir tetap sama sejumlah 20 digit.

Solusi lainnya adalah membuat sistem listrik prabayar secara online. Setiap meter listrik dapat terhubung dengan PLN melalui internet. Untuk membeli kuota listrik pelanggan hanya perlu membuka website PLN dan memasukkan jumlah listrik yang akan dibeli beserta nomor meternya. Kemudian uang pulsa dapat ditransfer. Token yang sudah dibuat dapat langsung dikirimkan ke meter listrik tujuan, tanpa perlu diubah menjadi 20 digit ataupun diberi tambahan pengaman lagi.

Untuk menjamin keamanan dapat juga dilakukan penggantian *decoder key* yang berkala dan terjadwal, tidak hanya saat terjadi perubahan parameter penyusun *decoder key*. Dengan perubahan berkala ini akan makin sulit melakukan serangan *brute force* terhadap kunci yang dibuat.

IV. KESIMPULAN DAN SARAN

AES dapat digunakan sebagai alternatif algoritma enkripsi token pada listrik prabayar. Selain karena terjamin keamanannya AES juga ringan komputasinya baik untuk software ataupun hardware. Meskipun begitu masih diperlukan penyempurnaan untuk mendapatkan token akhir yang lebih pendek. Selain itu penggunaan metode ini dapat dikembangkan untuk listrik prabayar online dengan decoder key yang rutin diubah agar lebih aman.

REFERENCES

[1] Kaplan, Roy (1995) STANDARD TRANSFER SPECIFICATION : Guidelines. Measurement and Control Departement Nasional PTM&C, Transmission Group, Eskom

[2] NRS Project (1997). NRS 009-6-9:1997. Rationalized User Specification, Electricity Sales System, Part 6, Section 9. South African Bureau of Standards.

[3] IEC (2007). IEC 62055-41 : Electricity metering payment system, Part 41 : STS – Application layer protocol for one-way token carrier systems.

[4] https://bruangku.wordpress.com/2011/03/16/listrik-prabayar-pln/ diakses terakhir pada 10 Mei 2015

[5] ww.sts.org.za diakses terakhir pada 10 Mei 2015

[6] www.eskom.co.za diakses terakhir pada 10 Mei 2015

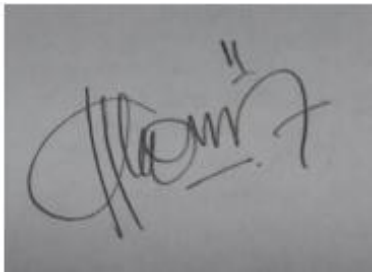
[7] http://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html diakses terakhir pada 10 Mei 2015

[8] Munir, Rinaldi (2015). Diktat kuliah IF4020 : Kriptografi. Informatika ITB

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, 11 Mei 2015



Khoirunnisa Afifah/13512077