JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI
INSTITUT TEKNOLOGI SEPULUH NOPEMBER

USULAN TUGAS AKHIR

1. IDENTITAS PENGUSUL

Nama : Yolanda Septiana Dewi
NRP : 5109100187
Dosen Wali : Dwi Sunaryono, S.Kom, M.Kom

2. JUDUL TUGAS AKHIR

Implementasi Skema *Digital Rights Management* dengan *Anonymous Trust* untuk Buku Audio di Perangkat Android

Implementation of Digital Rights Management Scheme with Anonymous Trust for Audio Book on Android Device

3. URAIAN SINGKAT

Salah satu isu pada penerapan *Digital Rights Management* (DRM) adalah dalam hal perlindungan data konsumen. Hasil penelitian yang dipublikasikan oleh *Canadian Internet Policy and Public Interest* (CIPPIC) milik *University of Ottawa* mengindikasikan bahwa DRM digunakan untuk mengumpulkan, menggunakan, dan membuka informasi personal milik konsumen untuk tujuan lain yang tidak berhubungan langsung dengan sistem DRM [1].

Sistem DRM seharusnya tidak merambah ke data konsumen, sebagaimana fungsinya untuk mengenkripsi media, membuat lisensi dan mengirimkan media dan lisensi tersebut ke konsumen. Namun pihak penerbit/pemasar yang memiliki data konsumen seringkali tidak memberitahu konsumen jika data kosumen tersebut digunakan untuk tujuan lain. Kekhawatiran terbesar adalah adanya pengumpulan data konsumen oleh pihak ketiga melalui penerbit/pemasar.

Untuk mencegah keterkaitan data konsumen pada sebuah sistem DRM, biasanya digunakan otentikasi oleh pihak ketiga yang dipercaya oleh kedua pihak (penerbit/pemasar maupun konsumen). Pihak ketiga tersebut wajib untuk menyimpan rahasia kedua pihak. Dalam tugas akhir diajukan ini sebuah skema DRM dengan *anonymous trust* yang tidak menggunakan pihak ketiga untuk proses otentikasi. Skema ini menggunakan *Anonymity ID* yang berbeda untuk mengakses konten yang berbeda. *Anonymity ID* dibuat oleh penyedia konten setelah konsumen melakukan mekanisme pembayaran terhadap konten dan dikirimkan kepada konsumen untuk membuka konten. Dengan adanya mekanisme DRM yang anonim, maka data konsumen tidak akan dapat ditelusuri dari sistem sehingga keamanannya terjamin. Selain itu, skema DRM dengan *anonymous trust* ini tidak melibatkan *Certificate Authority* untuk otentikasi seperti yang terdapat

pada skema OMA DRM 2.0 [3] sehingga memiliki biaya komputasi yang rendah dan dapat diimplementasikan pada perangkat bergerak.

Sistem DRM pada industri musik pada dekade terakhir sudah meredup [4]. Industri musik beralih pada metode *watermarking* dan bekerja sama langsung dengan penyedia jasa internet. Sementara penerapan DRM pada *games* dan buku elektronik masih ada hingga saat ini. Implementasi DRM pada tugas akhir ini adalah untuk buku audio karena buku audio mulai digemari oleh masyarakat dan lebih efisien daripada buku elektronik biasa.

Implementasi DRM pada tugas akhir ini diharapkan dapat membantu individu untuk memahami isu keamanan data konsumen pada DRM dan solusinya. Selain itu juga untuk membantu memahami penerapan DRM pada *file* audio seperti buku audio pada perangkat bergerak.

4. PENDAHULUAN

4.1 Latar Belakang

Digital Rights Management (DRM) adalah metode untuk memberikan kontrol akses terhadap suatu properti milik penerbit, pembuat perangkat keras, pemegang hak cipta, atau individu yang ingin membatasi penggunaan sebuah konten [5]. Penerapan DRM ditujukan untuk mengurangi aktivitas pembajakan pada sebuah konten, walaupun pada kenyataannya, DRM tidak begitu berhasil memerangi aktivitas tersebut.

Keberadaan DRM selalu ditentang oleh konsumen karena membuat konsumen tidak bebas untuk membuka dan membagikan konten kapan saja, dimana saja. Selain itu, sebagian besar DRM tidak melindungi data konsumen. Laporan hasil penelitian CIPPIC pada September 2007 sudah cukup membuktikan bahwa beberapa sistem DRM tidak dapat menjaga kerahasiaan data konsumen [6]. Laporan tersebut menyelidiki sistem DRM yang digunakan pada 16 produk dan layanan digital termasuk toko musik Apple iTunes, Microsoft Office Visio, dan Symantec North SystemWorks 2006.

Sementara penerapan DRM pada industri musik, iTunes telah menghapus DRM pada tahun 2009 demi kenyamanan konsumen, dan beralih pada *watermark* [4]. Begitupun pada sebagian industri buku elektronik juga tidak menerapkan DRM, meskipun perusahaan buku elektronik terbesar seperti Amazon masih mempertahankan DRM pada Kindle [6]. Perusahaan buku audio Audible milik Amazon juga diketahui masih menerapkan DRM pada buku audionya.

Sebagian besar keamanan dalam sistem DRM dicapai menggunakan metode "keamanan dengan penyembunyian" (*security by obscurity*) yaitu metode keamanan sistem dimana arsitektur dan desain sistem tersebut dirahasiakan oleh pembuat sistem. Namun terdapat beberapa metode DRM yang bersifat terbuka seperti OMA DRM yang merupakan sebuah standar DRM yang dibuat oleh beberapa perusahaan perangkat bergerak.

Oleh karena itu pada tugas akhir ini diajukan sebuah skema DRM yang dapat digunakan oleh konsumen tanpa memberikan data pribadi pada proses perolehan lisensi maupun proses pelacakan. Diharapkan skema ini dapat membantu individu untuk memahami

perancangan sistem DRM yang lebih aman dan penerapannya pada buku audio, walaupun skema ini tidak dapat menghilangkan ketidaknyamanan konsumen secara total, karena pada dasarnya penerapan DRM akan selalu membuat konsumen merasa dirugikan.

4.2 Rumusan Masalah

- Bagaimana cara merancang konsep *Digital Rights Management* menggunakan *anonymous trust* pada perangkat Android untuk menghilangkan keterkaitan data konsumen dengan sistem DRM?
- Bagaimana cara mengimplementasikan konsep *Digital Rights Management* menggunakan *anonymous trust* pada perangkat Android untuk menghilangkan keterkaitan data konsumen dengan sistem DRM?
- Bagaimana cara memainkan *file* audio yang menggunakan format DRM pada perangkat Android?

4.3 Batasan Masalah

1. Perangkat lunak dibangun untuk digunakan pada *platform* Android.
2. Skema DRM diterapkan untuk buku audio.
3. Skema DRM mengasumsikan terdapat pihak ketiga untuk proses pembayaran.

4.4 Tujuan dan Manfaat

Tujuan tugas akhir ini adalah

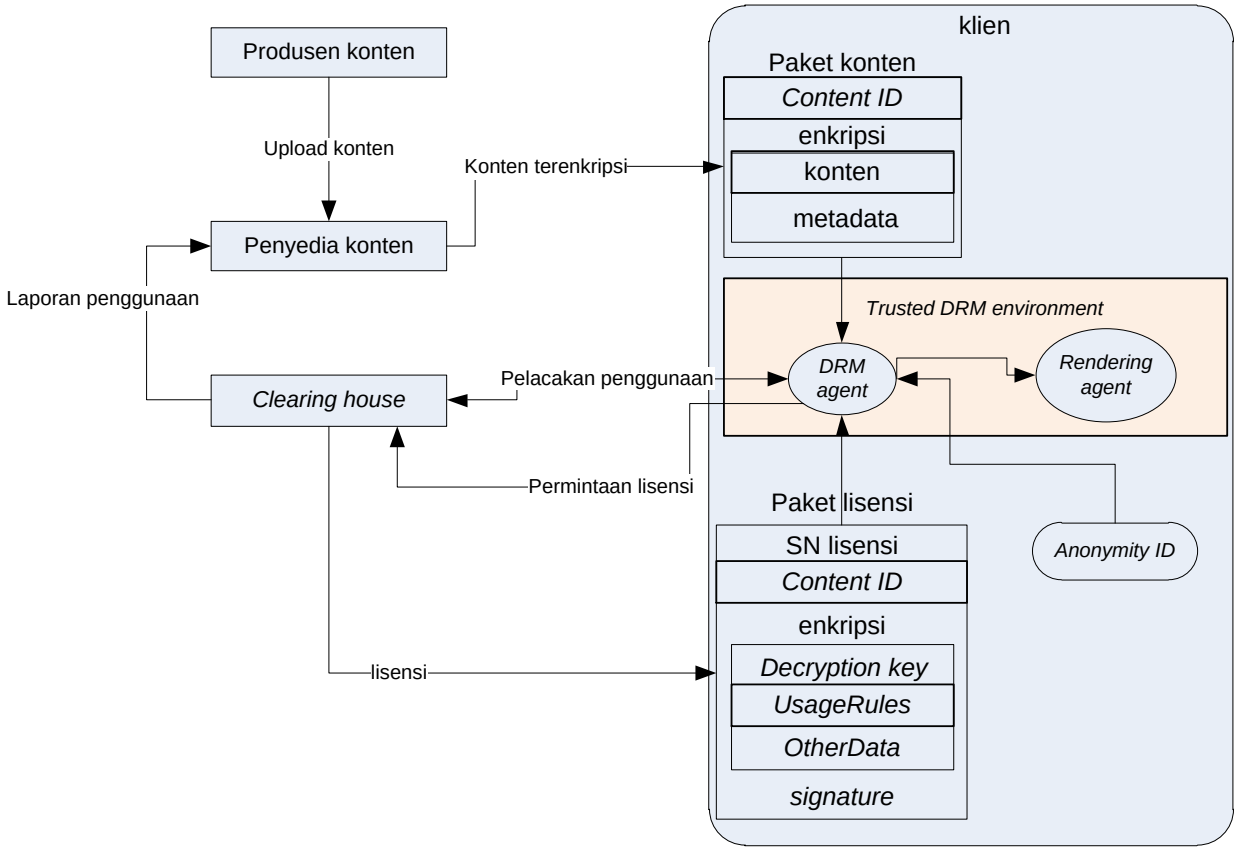
- Merancang konsep *Digital Rights Management* menggunakan *anonymous trust* pada perangkat Android untuk menghilangkan keterkaitan data konsumen dengan sistem DRM.
- Mengimplementasikan konsep *Digital Rights Management* menggunakan *anonymous trust* pada perangkat Android untuk menghilangkan keterkaitan data konsumen dengan sistem DRM.
- Memainkan *file* audio yang menggunakan format DRM pada perangkat Android.

Manfaat tugas akhir ini adalah terciptanya sebuah aplikasi yang menggunakan skema DRM yang aman karena tidak melibatkan data pribadi konsumen. Selain itu tugas akhir ini dapat dijadikan bahan kajian terhadap implementasi DRM secara anonim pada buku audio.

5. TINJAUAN PUSTAKA

Terdapat empat peran dalam rancangan skema DRM seperti yang tergambar pada Gambar 1, yaitu produsen konten, penyedia konten, *clearing house* (CH), dan klien yang memiliki *DRM agent* (DA). Produsen konten memiliki peran untuk membuat konten digital dan mengenkripsi menggunakan salah satu metode enkripsi, seperti RSA, ElGamal, atau ECC, kemudian mengirimkan konten yang telah terenkripsi ke penyedia konten. Klien meminta konten dari penyedia konten, lalu penyedia konten mengirimkan konten yang telah dienkripsi dan dibungkus dalam format khusus kepada klien. Konten yang diterima oleh klien tidak dapat digunakan tanpa lisensi yang valid dikarenakan oleh enkripsi. Ketika klien telah melakukan pembayaran dan memulai protokol perolehan lisensi dengan CH melalui DA, klien kemudian menerima lisensi

yang dapat digunakan untuk mendekripsi konten tersebut. CH bertugas untuk membuat dan mengirimkan lisensi yang diminta oleh klien dan mencatat laporan penggunaan konten yang diterima dari DA. Sementara DA berperan untuk mengeksekusi konten yang terenkripsi menggunakan *Anonymity ID* dan lisensi agar dapat dimainkan serta melaporkan catatan penggunaan konten kepada CH. DA terdapat pada perangkat yang digunakan oleh klien.



Gambar 1. Struktur sistem DRM [7]

Proses perolehan lisensi secara umum adalah sebagai berikut: klien membayar sejumlah biaya kepada penyedia konten, kemudian mendapatkan identitas anonim (*Anonymity ID*) dan nilai otentikasi $H(Anonymity\ ID \oplus X)$ untuk konten yang terenkripsi. Kemudian, penyedia konten mengirimkan *Anonymity ID*, $H(Anonymity\ ID \oplus X)$, dan *Content ID* ke CH. Selanjutnya, klien menggunakan *Anonymity ID* dan $H(Anonymity\ ID \oplus X)$ untuk diotentikasi oleh CH dan mendapatkan *decryption key* untuk konten.

Tabel 1. Notasi yang digunakan pada skema yang diajukan

Notasi	Penjelasan
$H(\ )$	Fungsi *hash* satu arah
SK	*Session key*
$E_{SK}(\cdot)$ / $D_{SK}(\cdot)$	Enkripsi/dekripsi simetrik dengan *session key* SK

X	*Secret key* dari penyedia konten
License	Lisensi konten digital
Anonymity ID	Identitas anonim klien
Content ID	Identitas konten digital
UsageRules	Aturan penggunaan konten digital
UsageData	Data penggunaan konten digital
||	Penggabungan string
SN	Nomor urut dari lisensi
$\oplus$	Operasi XOR
Decryption key	Kunci untuk mendekripsi konten digital yang terenkripsi
OtherData	Informasi tambahan pada lisensi

Tahap otentikasi dan perolehan lisensi [7]**:**

Pada tahap ini, klien telah mengunduh konten digital yang terenkripsi dan ingin mendapatkan lisensi dari CH untuk mengakses konten. CH mengotentikasi klien dan mengirimkan lisensi kepada klien yang valid. Langkah-langkah dalam tahap ini ditunjukkan sebagai berikut sesuai dengan notasi-notasi pada Tabel 1:

Langkah 1: DA memilih angka acak R_{DA} untuk menghitung nilai kunci sementara S_{DA} = $H(H(anonymity\ ID \oplus X)) \oplus R_{DA}$ dan $C_{DA} = H(R_{DA})$. Kemudian, DA mengirim *Anonymity ID*, S_{DA}, dan C_{DA} ke CH.

Langkah 2: CH menghitung $R'_{DA} = S_{DA} \oplus H(H(Anonymity\ ID \oplus X))$ untuk mengecek apakah C_{DA} sama dengan $C'_{DA} = H(R'_{DA})$. Jika kedua nilai sama, maka otentikasi DA valid. Kemudian, CH memilih angka acak R_{CH} untuk menghitung nilai $S_{CH} = H(H(Anonymity\ ID \oplus X) \| R_{DA}) \oplus R_{CH}$ dan *session key* $SK = H(H(Anonymity\ ID \oplus X) \| R_{DA} \| R_{CH})$. Terakhir, CH menghitung nilai $C_{CH} = H(R_{DA} \| R_{CH} \| SK)$ lalu mengirimkan S_{CH} dan C_{CH} ke DA.

Langkah 3: DA menghitung nilai $R'_{CH} = S_{CH} \oplus H(H(Anonymity\ ID \oplus X) \| R_{DA})$ dan *SK'* = $H(H(Anonymity\ ID \oplus X) \| R_{DA} \| R'_{CH})$. Kemudian DA menghitung nilai $C'_{CH} = H(R_{DA} \| R'_{CH} \| SK')$ untuk mengecek apakah C_{CH} bernilai sama dengan C'_{CH}. Jika bernilai sama, maka otentikasi CH dan *SK* keduanya valid. Selanjutnya, DA menghitung E_{SK} (*Anonymity ID* || *Content ID* || *UsageRules* || *SK*) lalu mengirimkannya ke CH.

Langkah 4: CH menghitung nilai *License* = {*SN* || *Content ID* || *UsageRules* || *Decryption Key* || *OtherData*}. Kemudian CH menghitung nilai E_{SK} (*License* || *SK*) dan mengirimkannya ke DA. Akhirnya, DA dapat menggunakan *SK* untuk mendekripsi E_{SK}(*License* || *SK*) dan mendapatkan *License*. Dengan demikian, klien mendapat *Decryption Key* dari *License* dan menggunakannya untun mendekripsi konten.

Tahap pelacakan penggunaan [7]**:**

Pada tahap ini, CH menerima laporan penggunaan konten dari DA. Untuk mencegah penipuan, CH perlu mengotentikasi validitas dari DA. Informasi laporan penggunaan juga perlu dienkripsi untuk melindungi data klien. Langkah-langkah pada tahap ini dijelaskan sebagai berikut sesuai dengan notasi-notasi pada Tabel 1:

Langkah 1: Pertama, CH memilih sebuah angka acak $\overline{R}_{CH}$ untuk menghitung $\overline{S}_{CH} = H(H(Anonymity\ ID \oplus X)) \oplus \overline{R}_{CH}$ dan $\overline{C}_{CH} = H(\overline{R}_{CH})$. Kemudian, CH mengirim *Anonymity ID*, $\overline{S}_{CH}$, dan $\overline{C}_{CH}$ ke DA.

Langkah 2: DA menghitung $\overline{R'}_{CH} = \overline{S}_{CH} \oplus H(H(Anonymity\ ID \oplus X))$ untuk mengecek apakah $\overline{C}_{CH}$ bernilai sama dengan $\overline{C'}_{CH} = H(\overline{R'}_{CH})$. Jika sama, maka otentikasi CH adalah valid. Kemudian, DA memilih angka acak $\overline{R}_{DA}$ untuk menghitung nilai $\overline{S}_{DA} = H(H(Anonymity\ ID \oplus X) \| \overline{R}_{CH}) \oplus \overline{R}_{DA}$ dan *session key* $\overline{SK} = H(H(Anonymity\ ID \oplus X) \| \overline{R}_{CH} \| \overline{R}_{DA})$. Selanjutnya, DA menghitung $\overline{C}_{DA} = H(\overline{R}_{CH} \| \overline{R}_{DA} \| \overline{SK})$ lalu mengirimkan $\overline{S}_{DA}$ dan $\overline{C}_{DA}$ ke CH.

Langkah 3: CH menghitung $\overline{R'}_{DA} = \overline{S}_{DA} \oplus H(H(Anonymity\ ID \oplus X) \| \overline{R}_{CH})$ dan *session key* $\overline{SK'} = H(H(Anonymity\ ID \oplus X) \| \overline{R}_{CH} \| \overline{R'}_{DA})$. Kemudian, CH menghitung nilai $\overline{C'}_{DA} = H(\overline{R}_{CH} \| \overline{R'}_{DA} \| \overline{SK'})$ untuk mengecek apakah $\overline{C}_{DA}$ bernilai sama dengan $\overline{C'}_{DA}$. Jika sama, maka otentikasi DA valid dan $\overline{SK}$ valid. Selanjutnya, CH menghitung $E_{\overline{SK}}$ (*Anonymity ID* || *Content ID* || *SN* || $\overline{SK}$) dan mengirimkannya ke DA.

Langkah 4: DA menghitung $E_{\overline{SK}}$ (*UsageData* || $\overline{SK}$) dan mengirimkannya ke CH. Akhirnya, CH dapat mendekripsi $E_{\overline{SK}}$ (*UsageData* || $\overline{SK}$) untuk mencatat penggunaan data.

Skema ini dirancang dengan menggunakan fungsi *hash* dan operasi XOR, sehingga biaya komputasi rendah dan dapat digunakan pada perangkat bergerak secara efisien.

Pada penerapan skema diatas di perangkat bergerak akan memiliki dua kelemahan. Pertama, karena tidak adanya metode *Sign in*, konsumen tidak boleh kehilangan *Anonymity ID*, karena menyebabkan konsumen harus melalui tahap pembayaran lagi untuk mendapatkan *Anonymity ID*. Hal ini tentu saja merugikan konsumen karena konsumen yang memiliki lebih dari satu perangkat Android tidak bisa memainkan konten pada perangkat yang berbeda. Kedua, *Anonymity ID* dan *License* tersimpan pada perangkat, jika *Anonymity ID* dan *License* didapatkan oleh klien lain yang tidak melakukan pembayaran terhadap konten, maka klien tersebut pada akhirnya dapat membuka konten pada perangkat yang berbeda.

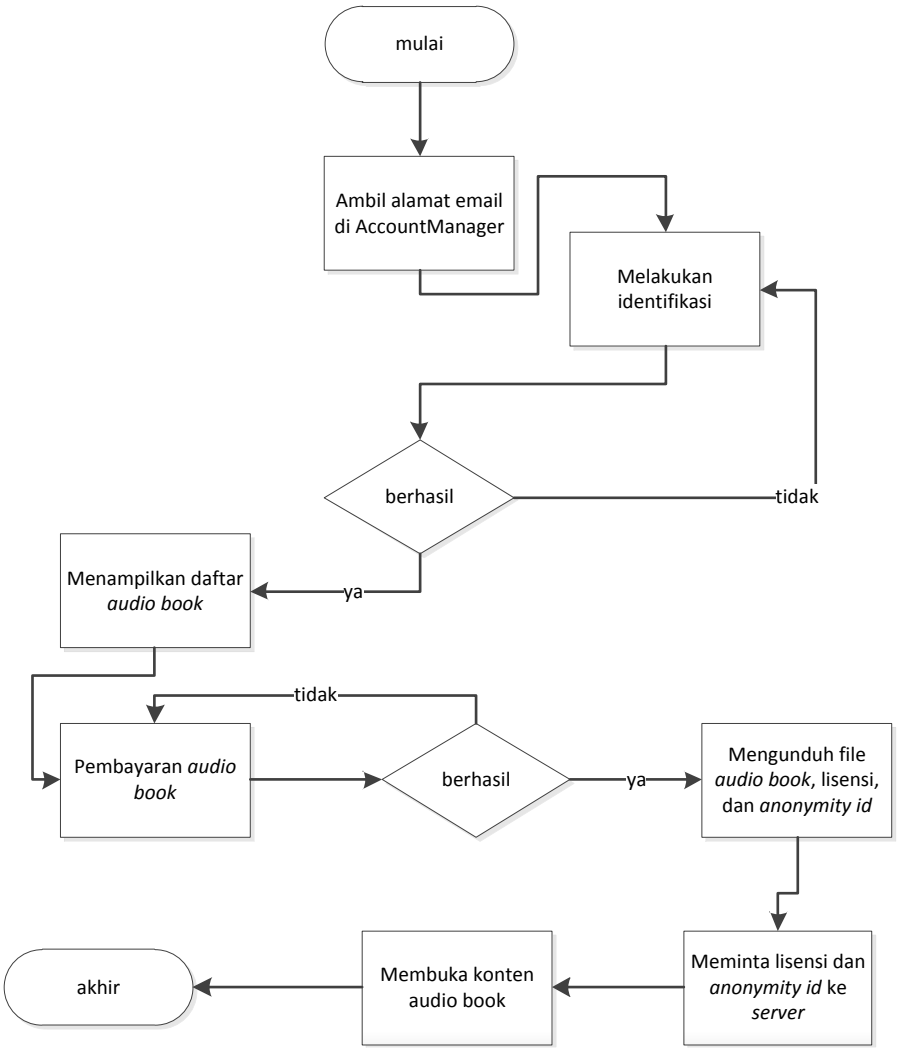
Oleh karena itu, sebagai tambahan, pada tugas akhir ini diajukan sebuah mekanisme agar sistem DRM dapat mengingat konsumen menggunakan alamat *email* yang sudah terdapat pada perangkat konsumen. Dengan metode ini, sistem DRM dapat mengambil daftar buku audio apa saja yang pernah dibeli oleh konsumen, juga memberikan lisensi kepada konsumen jika

konsumen kehilangan lisensi tersebut. Metode ini juga memberikan kebebasan kepada konsumen untuk memainkan buku audio pada lebih dari satu perangkat.

6. METODOLOGI

Sistem DRM yang diajukan memiliki rancangan fitur-fitur dan elemen-elemen yaitu, sebuah *server* yang bertugas untuk menyimpan *Anonymity ID* dan *License* milik tiap konsumen, pemberian konten dan lisensi, serta berisi sebuah aplikasi klien yang dapat melihat daftar buku audio, mengunduh konten dan lisensi dari *server*, dan memainkan buku audio tersebut.

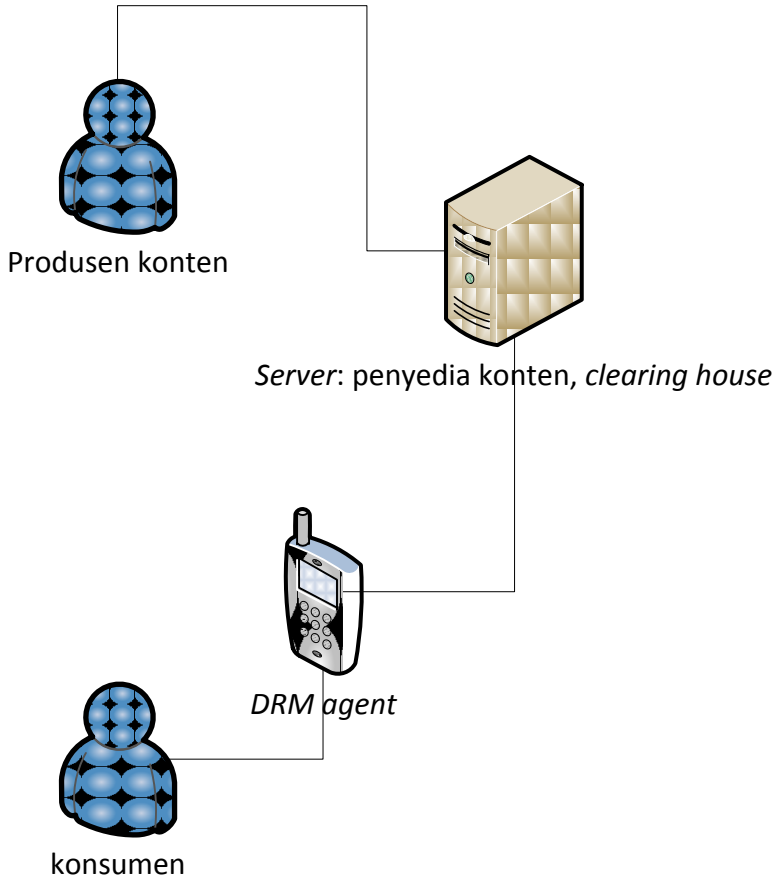
Aplikasi klien akan dirancang menggunakan Android SDK.



Gambar 2. *Flow chart* proses DRM pada *DRM agent*

Gambar 2 merepresentasikan proses yang dialami oleh *DRM Agent* (DA) dalam sistem DRM ini. Pertama, ketika membuka aplikasi, DA akan mengecek apakah konsumen mempunyai

alamat *email* yang tersimpan pada kelas `AccountManager` pada Android SDK. Kemudian DA akan menampilkan daftar buku audio yang tersedia. Jika konsumen ingin membeli buku audio, maka konsumen akan melalui tahap pembayaran (yang diasumsikan menggunakan pihak ketiga). Setelah itu DA akan mendapatkan lisensi dan *Anonymity ID* dan mengunduhnya serta konten buku audio. Terakhir, DA mengekstrak *decryption key* dari lisensi dan mendekripsi konten sehingga dapat didengar oleh konsumen.



Gambar 3. Arsitektur DRM

Gambar 3 menjelaskan secara umum tentang arsitektur sistem DRM yang diajukan. Entitas-entitas yang terlibat antara lain: produsen konten, penyedia konten, *clearing house*, dan konsumen atau klien. Fungsi masing-masing entitas telah dijelaskan pada bab Tinjauan Pustaka.

7. JADWAL KEGIATAN

No.	Tahapan	Bulan															
		Maret				April				Mei				Juni			
1.	Penyusunan proposal																
2.	Studi literatur																
3.	Perancangan sistem																
4.	Implementasi																
5.	Pengujian dan evaluasi																
6.	Penyusunan buku tugas akhir																

8. DAFTAR PUSTAKA

[1] Rafael Ruffolo. (2007, September) Study Says DRM Violates Canadian Privacy Law. Web Page. [Online]. http://www.pcworld.com/article/137404/article.html

[2] Wikipedia. (2010, September) OMA DRM. Web Page. [Online]. http://en.wikipedia.org/wiki/OMA_DRM

[3] Cyrus Farivar. (2012, December) The Music Industry Dropped DRM Years Ago. So Why Does It Persist on Ebooks? Web Page. [Online]. http://arstechnica.com/business/2012/12/the-music-industry-dropped-drm-years-ago-so-why-does-it-persist-on-e-books/

[4] Wikipedia. (2013, March) Digital Rights Management. Web Page. [Online]. http://en.wikipedia.org/wiki/Digital_rights_management

[5] Canadian Internet Policy and Public Interest Clinic, "Digital Rights Management Technologies and Consumer Privacy," University of Ottawa, Ottawa, Study ISBN, 2007.

[6] Erez Zukerman. (2012, December) How to Break The DRM on Kindle Ebooks So You Can Enjoy Them Anywhere. Web Page. [Online]. http://www.makeuseof.com/tag/how-to-break-the-drm-on-kindle-ebooks-so-you-can-enjoy-them-anywhere/

[7] Jen-Ho Yang, Chih-Cheng Hsueh, and Chung-Hsuan Sun, "An Efficient and Flexible Authentication Scheme with User Anonymoty for Digital Right Management," in *Fourth International Conference on Genetic and Evolutionary Computing*, Shenzhen, China, 2010.