

**Tugas EC 7010  
Keamanan Sistem Lanjut**

**Otentifikasi dan Otorisasi pada  
*Mobile Environment***

*oleh*

**Herry Herlambang  
NIM. 232 03 144**



**PROGRAM MAGISTER TEKNIK ELEKTRO  
BIDANG KHUSUS TEKNOLOGI INFORMASI  
INSTITUT TEKNOLOGI BANDUNG  
2004**

## Daftar Isi

<b>Daftar Isi</b> .....	1
<b>Abstrak</b> .....	2
<b>BAB I PENDAHULUAN</b> .....	3
1.1 Latar Belakang .....	3
1.2 Pembatasan Masalah .....	3
1.3 Tujuan .....	3
1.4 Singkatan yang Digunakan .....	4
<b>BAB II DEFENISI</b> .....	5
2.1 Otentifikasi .....	5
2.2 Otorisasi .....	5
2.3 <i>Mobile Environment</i> .....	5
2.4 <i>Public Key Infrastructure</i> dan <i>Public Key Cryptography</i> .....	5
2.5 <i>Certificate Authorities</i> dan <i>Digital Certificates</i> .....	6
2.6 SPKI – <i>Simple Public Key Infrastructure</i> .....	7
2.7 X.509 PKI .....	7
<b>BAB III KEBUTUHAN DAN METODA OTENTIFIKASI DAN OTORISASI</b> .....	8
3.1 Kebutuhan untuk Otentifikasi dan Otorisasi .....	8
3.2 Metoda pada Otentifikasi dan Otorisasi .....	9
3.2.1 <i>Password</i> .....	9
3.2.2 <i>Password</i> dengan Tanda( <i>Token</i> ) .....	9
3.2.3 <i>Biometrics</i> .....	10
3.2.4 <i>Digital Signatures</i> .....	10
3.2.5 Karakteristik Mekanisme Otentifikasi dan Otorisasi yang Baik .....	11
<b>BAB IV TEKNIK, STANDAR DAN MEKANISME OTENTIFIKASI DAN OTORISASI     PADA MOBILE ENVIRONMENT</b> .....	13
4.1 Kemampuan Secara Teknis yang Dimiliki oleh Mobile Device sekarang .....	13
4.1.1 <i>Wireless Transport Layer Security</i> .....	13
4.1.2 <i>Wireless Identity Module</i> .....	14
4.2 Standar Pada Mobile Environment .....	15
4.2.1 Metoda Sedarhana .....	15
4.2.2 Produk yang ada Dipasar .....	15
4.3 Mekanisme Otentifikasi dan Otorisasi Secara Universal .....	16
<b>BAB V KESIMPULAN</b> .....	20
<b>DAFTAR PUSTAKA</b> .....	21

## Abstrak

Pada aplikasi yang informasinya dapat diakses melalui jaringan (*network*), seperti *electronic banking*, validasi/otentifikasi identitas *user* dan otorisasi merupakan permasalahan utama yang dihadapi aplikasi ini.

Ada banyak mekanisme untuk menjalankan otentifikasi dan otorisasi, ada yang menyediakan tingkat keamanan yang tinggi dan ada juga yang mudah digunakan oleh pengguna. *Public Key Infrastructure* (PKI) merupakan aplikasi yang secara umum dianggap paling aman dan dapat diandalkan.

Pada lingkungan *mobile*, dimana suatu *service* dapat akses melalui kanal yang berbeda, seperti web dan WAP, permasalahan otentifikasi dan otorisasi menjadi lebih rumit. Misalnya dapatkah *private key* yang diatur PKI digunakan pada platform yang berbeda.

Perkembangan standarisasi teknologi informasi dengan cepat dan dengan kecepatan yang tetap dapat mempercepat pemecahan masalah otentifikasi dan otorisasi. Penerapan teknologi otentifikasi dan otorisasi ini selangkah tertinggal jika dibandingkan dengan perkembangannya.

**Kata Kunci** : Otentifikasi, Otorisasi, *Mobile Environment*, PKI

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

Pada saat membangun suatu aplikasi yang dapat diakses melalui internet, otentifikasi identitas dan otorisasi *user* menjadi masalah utama yang dihadapi oleh pengembang. Otentifikasi dan otorisasi dengan tingkat kepercayaan yang sangat tinggi sangat diperlukan. Hal ini dikarenakan internet bersifat terbuka dan tidak dapat dipercaya (*unreliable*). Banyak skema yang dikembangkan untuk mendapatkan tingkat otentifikasi dan otorisasi yang sesuai dengan yang diinginkan, beberapa skema lebih baik dari yang lain dari segi *user friendliness*, tingkat kepercayaan dan keamanan.

Pada era *mobile internet* sekarang ini, prosedur otentifikasi dan otorisasi mulai difikirkan kembali karena adanya perbedaan mekanisme otentifikasi dan otorisasi dengan *fix location*. Masalah yang dihadapi adalah harus ada suatu mekanisme yang senyaman mungkin bagi *user* dan memberikan tingkat kepercayaan yang tinggi sebagai hasil dari suatu proses otentifikasi.

### 1.2 Batasan Masalah

Pembatasan masalah pada tulisan ini adalah :

1. tulisan ini membahas tentang metoda yang saat ini digunakan untuk otentifikasi dan otorisasi pada *mobile environment*,
2. tulisan ini tidak terfokus hanya pada aplikasi wireless, tetapi pada pengertian yang lebih luas dari *mobile environment* (sub bab 2.3),
3. pembahasan disini difokuskan pada pemecahan masalah dengan menggunakan PKI, walaupun metode otentifikasi lain juga dibahas,
4. tulisan ini juga membahas beberapa isu, seperti *Public Key Cryptography*.

### 1.3 Tujuan

Tujuan dari tulisan ini adalah :

1. tujuan dari pembuatan tulisan ini adalah untuk memperjelas konsep otentifikasi dan otorisasi serta membahas bagaimana konsep dan prosedur yang berkaitan dengannya dapat diterapkan atau digunakan pada *mobile environment*,
2. pada tulisan ini juga akan memuat satu protokol atotentifikasi baru, yang sesuai dengan teknologi yang dibahas pada tulisan ini.

#### **1.4 Singkatatan yang Digunakan**

ACL	<i>Access Control List</i>
ATM	<i>Automatic Time Machine</i>
CA	<i>Certificate Authority</i>
DA	<i>Digital Certificates</i>
eCommerce	<i>Electronic Commerce - Commerce transactions carried out in information networks</i>
eStore	<i>Electronic Store - A website where one can perform eCommerce transactions</i>
RFC	<i>Request For Comments</i>
ME	<i>Mobile Entity, Mobile Equipment</i>
MeT	<i>Mobile Electronic Transactions Initiative</i>
MSISDN number	<i>Mobile Subscriber Integrated Services Digital Network Number</i>
PIN	<i>Personal Identification Number</i>
PKI	<i>Public Key Infrastructure</i>
PKC	<i>Public Key Cryptography</i>
SIM	<i>Subscriber Identity Module</i>
SPKI	<i>Simple Public Key Infrastructure</i>
SSL	<i>Secure Sockets Layer</i>
WAP	<i>Wireless Application Protocol</i>
WIM	<i>Wireless Identity Module</i>
WTLS	<i>Wireless Transport Layer Security</i>

## **BAB II**

### **DEFENISI**

#### **2.1 Otentifikasi**

Otentifikasi merupakan proses untuk menentukan apakah seseorang atau sesuatu sesuai dengan yang diakuinya atau yang dinyatakannya[5].

Ada lima metoda dalam otentifikasi yaitu [5]:

1. Sesuatu yang mengakui mengetahui (Something the claimant knows),
2. Sesuatu yang mengakui memiliki (Something the claimant owns),
3. Sesuatu yang mengakuinya (Something the claimant is),
4. Pengakuan pada tempat atau waktu tertentu (Claimant is at a particular place (at a particular time)),
5. Otentifikasi diterbitkan oleh pihak ketiga yang terpercaya (Authentication is established by a trusted third party).

#### **2.2 Otorisasi**

Otorisasi merupakan suatu proses untuk memberikan izin kepada seseorang untuk melakukan atau memberikan sesuatu. Hal ini berarti untuk membuat seseorang dapat mengakses sesuatu, orang tersebut harus terlebih dahulu diotentifikasi terlebih dahulu. Dengan kata lain otentifikasi dikerjakan terlebih dahulu sebelum otorisasi. Sebenarnya otentifikasi dari suatu entiti atau identitas, tidak selalu diperlukan dalam otorisasi, jika otorisasi dapat divalidasi dengan cara lain. (sub bab 2.6).

#### **2.3 Mobile Environment**

Dalam konteks tulisan ini, mobile environment adalah suatu setting atau pengaturan dimana *user* dapat mengakses sistem melalui internet atau jaringan terbuka lainnya, yang tidak terikat dengan tempat, peralatan atau kanal akses dalam rangka mendapatkan *servis* dari sistem. Contoh dari pengaturan ini pada sistem sistem perbankan yang dapat diakses melalui internet atau WAP.

#### **2.4 Public Key Infrastructure(PKI) dan Public Key Cryptography(PKC)**

PKI adalah suatu sistem untuk memberitahukan nilai *public-key* yang digunakan pada PKC [2]. PKC diperkenalkan pertamakali oleh Diffie dan Hellman pada tahun 1976 [3]. PKC

merupakan perhitungan matematika yang kompleks dimana perhitungan ini menggunakan bilangan prima, oleh karena itu tidaklah mungkin dapat dipecahkan dengan mudah tanpa menggunakan input yang tepat, input yang tepat ini adalah kunci yang digunakan. PKC terdiri dari dua buah kunci yaitu :

1. *Private Key*

Kunci ini dirahasiakan oleh pemilik kunci

2. *Public Key*

Kunci ini diberikan kepada masyarakat umum.

dimanan antara kedua kunci tidak ada hubungan sehingga apabila seseorang telah memiliki *public key* dia tidak dapat untuk menggunkanya untuk mengetahui *private key*. Data yang dienkripsi dengan menggunakan *public key* hanya dapat didekripsi dengan menggunakan *private key* atau sebaliknya. Pada tulisan ini tidak membahas PKC dan algoritma yang terkait dengan PKC secara detail.

Ada banyak cara dalam mengimplementasikan PKI, tetapi ada dua hal yang selalu ada dalam implementasi PKI yaitu :

- ▶ **Sertifikasi**, merupakan proses untuk mengintegrasikan nilai public key dengan individu atau atribut.
- ▶ **Validasi**, merupakan proses untuk memastikan kebenaran dari sesuatu.

Permasalahan utama yang harus dapat dipecahkan oleh PKI dan PKC adalah sistem implemtasinya, dimana dititik beratkan pada manajemen *private key*. Kunci ini harus tetap dirahasiakan dan pengguna kunci ini tetap mempunyai akses terhadapnya.

## **2.5 Certificate Authorities(CA) dan Digital Certificates(DC)**

CA merupakan suatu lembaga atau organisasi yang menyatakan kebenaran dan menerbitkan DA. DA merupakan data yang terdiri dari *public key* dan atributnya yang berisikan keterangan dari pemilik dan identitas dari CA. Sertifikat yang diterbitkan oleh CA memungkinkan seseorang untuk menandai sesuatu dengan publik keynya dan penandaan ini dapat dibuktikan kebenarannya dengan adanya identitas dan tanda dari CA. Hal ini dapat terjadi karena penerbit CA merupakan lembaga yang terpaca.

Pada PKI juga terdapat jaringan atau hirarki dari CA [2, 6], oleh karena itu memungkinkan suatu CA dipercayai, maka akan dipercayai juga oleh yang CA yang lain.

## 2.6 SPKI – *Simple Public Key Infrastructure*

SPKI didefinisikan pada IETF RFC 2693 [4]. Ide dasar dari sertifikat SKPI berhubungan dengan pihak yang berwenang mengeluarkan kunci. Konsep ini berbeda dengan PKI, dimana pada PKI identifikasi dari kunci terdapat pada sertifikat. Dengan kata lain sertifikat SPKI lebih difokuskan pada hak yang mengikat (*binding rights*) dengan pihak yang berwenang mengeluarkan kunci, dari pada identifikasi kunci secara individual. Adapun implementasi dari konsep konvensional PKI diterapkan pada standar X.509 [4, 9].

Pada lingkungan yang terbuka SPKI lebih tepat dan aman digunakan karena sistem ini menyediakan pengaturan kerahasiaan dari pengguna, apabila pengguna telah mendapatkan sertifikat SPKI maka ia dapat mengakses *service* dan sumber daya tanpa harus membuka identitasnya. Kepercayaan didasarkan pada jaringan yang terpercaya dan otentifikasi yang terpercaya. Meskipun SPKI ini sangat ideal untuk diterapkan pada lingkungan terbuka, tetapi sayangnya produk yang ada di pasar belum dapat mendukung sistem ini [9].

## 2.7 X.509 PKI

X.509 merupakan standar PKI yang paling banyak digunakan. X.509 mendefinisikan aspek infrastruktur, seperti struktur sertifikat dan hirarki hubungannya dengan CA.

Dalam sertifikat X.509 memuat hal-hal berikut [9]:

<i>Version</i> , menjelaskan versi enkripsi sertifikat ( <i>encoded certificate</i> )
<i>Serial number</i> , merupakan identifikasi yang unik dari CA
<i>Issuer name</i> , merupakan identitas pihak yang mengeluarkan sertifikat
<i>Validity</i> , menunjukkan berapa jangka waktu sertifikat itu berlaku
<i>Subject identifying</i> , merupakan identitas dari pemegang <i>private key</i>
<i>Subject public key information</i>
<i>Issuer unique identifier</i>
<i>Subject unique identifier</i>
<i>Extensions field(s)</i>

Adapun versi terakhir dari standar X.509 adalah X.509v3

## BAB III

### KEBUTUHAN DAN METODA OTENTIFIKASI DAN OTORISASI

#### 3.1 Kebutuhan untuk Otentifikasi dan Otorisasi

Otentifikasi dari identitas seseorang atau sesuatu harus dilakukan untuk memastikan kebenaran identitas seseorang atau sesuatu. Hal ini dilakukan pada saat pengambilan keputusan apakah seseorang atau sesuatu diperbolehkan melakukan atau mendapatkan sesuatu.

Misalnya pada saat seseorang datang ke sebuah bank untuk mengambil uang, maka kasir pertama kali mengecek identitas dari nasabah tersebut misalnya dengan meminta kartu identitasnya. Kemudian kasir akan mengecek jumlah saldo dari nasabah tersebut untuk mengetahui seberapa besar nasabah berhak untuk mengambil uangnya. Setelah uang diperoleh oleh nasabah yang berbentuk uang kertas (*bank notes*) maka uang itu dapat dipergunakan sebagai alat pembayaran yang sah tanpa harus mengecek identitas orang yang menggunakannya. Mekanisme yang dilakukan diatas sangat menguntungkan bagi semua pihak karena :

1. setiap konsumen mempunyai hak privasi,
2. identitas konsumen tidak perlu diotentifikasi setiap akan melakukan pembayaran, hal ini menyebabkan transaksi dapat dilakukan dengan lebih cepat dan mudah,
3. pemerintah (*authorities*) yang mengeluarkan uang tidak secara langsung berhubungan dengan konsumen.

Prinsip diatas juga digunakan pada network. Atorisasi tidak diperlukan pada suatu servis yang dapat diakses oleh setiap orang. Berdasarkan teori, jika setidaknya ada satu orang harus diotentifikasi untuk mendapat *service* dan sumber daya tertentu, maka semua orang harus divalidasi sebelum diizinkan untuk mengakses *service* dan sumber daya.

Otentifikasi dari identitas seseorang diperlukan setiap saat identitas itu digunakan, seperti pada *eCommers*. Pada saat ini kebanyakan *eStore* pada internet, melakukan otentifikasi terhadap identitas pengguna sebelum berbelanja. *eStroe* melakukan otentifikasi jika kartu kredit yang digunakan telah dijamin oleh pihak lain. Aplikasi ini seharusnya dapat diterapkan pada *e-world*, karena setiap orang berhak terhadap privasinya, otentifikasi merupakan jalan terakhir dilakukan jika cara lain tidak dapat untuk memastikan identitas seseorang. Ada banyak metoda yang dikembangkan dalam menjamin keamanan uang elektronik (*e-money*) yang digunakan pada internet, metoda ini melakukan otentifikasi tanpa mengurangi privasi.[8, 9]

## 3.2 Metoda pada Otentifikasi dan Otorisasi

Pada sub bab ini akan dibahas metoda atau proses yang digunakan pada otentifikasi suatu identitas pengguna. Metoda yang digunakan menggunakan satu atau lebih dari karakteristik yang telah dijelaskan pada sub bab 2.1.

### 3.1.1 *Password*

*Password* diasosiasikan dengan nama pengguna yang merupakan cara yang paling mudah untuk otentifikasi. *Password* dapat mempunyai hubungan *one-to-one* atau *one-to-many* untuk setiap orang, oleh karena itu setiap pengguna dalam suatu sistem bisa memiliki *password* yang berbeda atau satu kelompok (*group*) dapat mempunyai *password* yang sama. Implementasi dari sistem yang menggunakan *password* sebagai cara untuk otentifikasi tidak lah terlalu rumit, yang diperlukan suatu tempat penyimpanan yang aman.

Kelamahan penggunaan *password* sebagai metoda otentifikasi adalah *password* sangat rentan terhadap serangan (*attacks*). Setidaknya tipe-tipe serangan seperti berikut yang dapat dilakukan pada *password* :

1. *external disclosure*,
2. *guessing*,
3. *communications eavesdropping*,
4. *replay attacks and host compromise* [5].

Ada beberapa skema yang dikombinasikan dengan password untuk dapat meningkatkan keamanannya diantaranya adalah *one-time-password*. Metoda ini memberikan sejumlah urutan *password* melalui kanal yang aman, *password* ini hanya dapat digunakan satu kali saja untuk mengotentifikasi kedalam sistem. Dengan menggunakan metoda ini telah menghilangkan kemungkinan *communications eavesdropping* dan *replay attacks*.

### 3.1.2 *Password dengan Tanda(Token)*

Password dapat dikombinasikan dengan objek fisik (sesuatu yang dimiliki oleh *user*) misalnya kartu ATM dengan *Personal Identification Number* (PIN), kartu ATM tanpa PIN atau sebaliknya maka masing-masingnya tidak ada gunanya.

Konsep ini dikembangkan lagi dengan menggunakan *integrated circuit cards* (ICC) or *smart card*. ICC merupakan suatu alat (*tamper proff device*) yang langsung berhubungan dengan alat lain, misalnya *SIM-card* pada *GSM-phones*.

'*Synchronous one-time passwords*' [5] merupakan metoda yang hampir sama dimana alatnya (*tamper proff device*) mengeluarkan kode yang dapat dijadikan sebagai *password*, yang

biasanya dikombinasikan lagi dengan PIN dan nama *user* untuk menghasilkan metoda otentifikasi *triplet*. Kode ini dihasilkan dengan menggunakan algoritma yang dinamakan *authenticator*, dengan menggunakan *authenticator* maka akan menghilangkan daftar password pada skema *one-time-password*.

### 3.1.3 Biometrik

Teknik otentifikasi dengan menggunakan biometrik terdiri dari :

1. *fingerprint recognition*,
2. *retinal scanning*,
3. *handgeometry scanning*
4. *handwriting and voice recognition* [5].

kelima teknik diatas didasarkan pada ciri-ciri fisik yang dimiliki oleh seseorang atau sesuatu.

Tiap-tiap individu memiliki ciri-ciri fisik yang berbeda walaupun perbedaan ini sangat tipis. Dengan perbedaan ini dapat dibedakan antara satu dengan yang lainnya walaupun pada saat-saat tertentu sangat sulit untuk mendapatkan tingkat otentifikasi yang sangat terpercaya. Lagipula teknologi yang tersedia sangat terbatas dan walaupun ada harganya sangat mahal. Pada beberapa aplikasi teknik ini dapat digunakan dengan baik tetapi pada lingkungan terbuka masih sangat sulit untuk diterapkan.

### 3.1.4 Digital Signatures

*Digital Signatures* digunakan untuk mengotentifikasi user pada PKI. Berikut ini ada beberapa tahapan yang digunakan untuk mengotentifikasi user dengan menggunakan *Digital Signatures* yaitu :

1. *user* meminta hak akses ke *service* atau sistem,
2. sistem membuat (*generates*) data untuk *user*, kemudian data tersebut dienkripsi dengan *private key*, setelah data tersebut dienkripsi kemudian data tersebut dikirim ke *user*,
3. *user* akan menghubungkan (*concatenates*) data yang diterima dari sistem, melakukan *a time stamp* dan mengenkripsi seluruh urutannya. (merupakan implementasi yang baik jika *a time stamp* dihubungkan (*concatenated*) dengan data, sehingga data yang akan dienkripsi tidak dapat secara lengkap diambil oleh pihak ketiga. *Hal ini* dapat menghindari kemungkinan terjadinya '*Chosen plain-text attack*' seperti yang dijelaskan pada [12].) kemudian data yang telah dienkripsi (*the cipher text*) akan dikirim kembali ke sistem bersama dengan hubungan (*link*) ke sertifikat atau sertifikat itu sendiri,

4. sistem akan mendekripsi informasi yang diterima dari *user* dengan menggunakan *public key* dari *user* yang terdapat pada sertifikat,
5. sistem akan memverifikasi informasi dari hasil dekripsi dengan data asli yang dibuat oleh sistem (nomor 1) dan validnya *a time stamp*. Jika sama maka sistem telah berhasil mengotentifikasi *user*.

### 3.1.5 Karakteristik Mekanisme Otentifikasi dan Otorisasi yang Baik

Pada sub bab ini akan dibahas karakteristik dari Otentifikasi dan Otorisasi yang Baik.

#### ► Kebenaran (*Correctness*)

Hasil dari setiap otentifikasi dan otorisasi haruslah tepat dan akurat. Jika memungkinkan otentifikasi user haruslah menghasilkan sesuatu, baik user terbukti seperti yang diakuinya maupun tidak. Berdasarkan kebenaran otentifikasi ini maka pada masa yang akan datang memungkinkan *user* atau kelompok dimana user terdaftar untuk mendapat kan *services* dan sumber daya

Pada kenyataannya sangatlah tidak mungkin untuk mendapatkan tingkat otentifikasi yang benar-benar terpercaya tetapi kepercayaan itu hanya pada tingkatan yang layak.

#### ► Kemungkinan untuk anonim dan privasi (*Possibility to anonymity and privacy*)

Otentifikasi terhadap suatu identitas hanya dilakukan apabila benar-benar diperlukan saja. Jika memungkinkan otorisasi dapat dilakukan tanpa harus membuka identitas *user*.

#### ► Kecepatan (*Speed*)

Proses otentifikasi seharusnya dilakukan dengan cepat, *user* dapat mendapatkan hasil dari proses otentifikasi ini salama satu atau dua detik.

#### ► Ketahanan terhadap serangan (*Attack resistance*)

Mekanisme otentifikasi seharusnya dapat tahan terhadap jenis serangan baik yang telah diketahui ataupun belum diketahui.

#### ► Murah (*Inexpensiveness*)

Mekanisme otentifikasi seharusnya memerlukan investasi yang luas salah satunya user atau alat otentifikasi

#### ► *User friendliness*

Mekanisme otentifikasi sedapat mungkin mudah digunakan dan dimengerti. Pada situasi yang maksimal, user tidak harus melakukan sesuatu untuk diotentifikasi. *User* seharusnya membawa suatu peralatan seperti *magnetic* atau *smart cards*, daftar *password* atau objek fisik lain dalam rangka otentifikasi user oleh sistem.

► **Universal (*Universality*)**

Sedapat mungkin user dapat menggunakan metoda otentifikasi yang sama pada semua service dan dimana saja.

**BAB IV**  
**TEKNIK, STANDAR DAN MEKANISME OTENTIFIKASI DAN OTORISASI**  
**PADA MOBILE ENVIRONMENT**

**4.1 Kemampuan Secara Teknis yang Dimiliki oleh Mobile Device sekarang**

Pada saat ini telepon seluler yang dapat mengakses ke internet, jumlahnya relatif terbatas ada dipasaran. Yang dimaksud dengan “telepon seluler dapat mengases internet” ini berarti telepon seluler telah dilengkapi dengan WAP. Telepon seluler pertama dipasaran yang telah dilengkapi dengan WAP ini adalah Nokia 7110, Ericsson dengan R320 kemudian banyak vendor HP yang menyusul. Pada yang sedikit model dan versi ini, WAP browsers yang digunakan adalah WTLS.

**4.1.1 Wireless Transport Layer Security (WTLS)**

WTSL merupakan suatu protokol yang digunakan pada WAP, dimana WTSL ini disusun oleh WAP Forum Initiative. Tujuan dari penyusunan WTSL ini adalah : “untuk menyediakan privasi, data integrity dan otentifikasi komunikasi antara dua aplikasi”[14].

Prtokol *handsahake* pada WTLS menciptakan hubungan yang aman antara *client* dan *server*. Protokol ini juga memberikan kemampuan server untuk mengotentifikasikan dirinya sendiri untuk diketahui oleh *client* dengan cara mengirimkan sertifikat atau hubungan kesertifikatnya, mekanisme ini juga berlaku kebalikannya[14]. Tabel berikut ini merupakan Prtokol *handsahake* pada WTLS. Bagian yang ditandai dengan asterisk (\*) sifatnya opsional.

Client	Server
ClientHello	---->
	ServerHello
	Certificate *
	ServerKeyExchange *
	CertificateRequest *
	<--- ServerHelloDone
Certificate *	
ClientKeyExchange *	
CertificateVerify *	
[ChangeCipherSpec]	
Finished	---->
	[ChangeCipherSpec]
	<--- Finished
Application Data	<---> Application Data

Tabel 1 : Prtokol *handsahake* pada WTLS [14]

Sepesifikasi WTLS tidak membutuhkan otentifikasi terhadap dirinya sendiri tetapi setiap client yang akan mengakses *services* akan diotentifikasi dengan menggunakan sertifikat yang dimilikinya. Pada kenyataannya pada telepon seluler, WAP *browser* dan SIM *cards* tidak memiliki sertifikat yang layak untuk otentifikasi. Dalam rangka standarisasi sertifikat dan *private key* pada WAP terminal, pada WAP Forum diperkenalkan “*Wireless Identifikasi Module Specification*”[13] sebagai santandar baru pada lingkungan WAP.

Tingkat keamanan yang bisa dijanjikan oleh WTLS sampai saat ini masih diperdebatkan. Enkripsi dan otentifikasi pada user antara WAP *gateway* dan *mobile equipment* tidak dilakukan terhadap keseluruhan *services* pada server. Hal ini bearti ada kesenjangan keamanan pada WAP *gateway* (data yang ada dalam bentuk *clear text* dan terintegrasi). Proses otentifikasi dan handshake merupakan proses yang terstandarisasi dari ujung ke ujung (*end-to-end*).

#### 4.1.2 Wireless Identity Module (WIM)

WIM didefenisikan pada WAP forum sebagai “suatu alat yang berupa *tamper resistant* yang digunakan untuk “mengoperasika WTLS, aplikasi fungsi keamanan dan yang paling penting untuk menyimpan dan memproses informasi yang dibutuhkan identifikasi dan otentifikasi *user*” [13]. WIM dirancang untuk diimplementasikan pada smartcard ataupun pada SIM.

WIM pada digunakan untuk [13]:

- ▶ Menyimpan sertifikat *private key* yang permanen (*private key* tidak pernah keluar dari WIM),
- ▶ Menyimpan serifikat *client* atau linknya,
- ▶ Menjalankan operasi *criptografi* selama *handshake* pada WTLS, terutama diperlukan otentifikasi *client*,
- ▶ Menandai data dengan *private key* untuk tujuan aplikasi,
- ▶ ‘*Unwarp*’ (data kunci yang ditandai dengan *public key* yang digunakan sebagai *private key* pada WIM),
- ▶ menyimpan sertifikat CA (dapat berubah),
- ▶ membuat angka yang acak yang digunakan untuk *criptografi*.

dapat dikatakan bahwa WIM memegang peranan penting dalam WTLS, tanpa adanya WIM mekanisme penanganan kunci, serifikat dan *signing operations* tidak dapat diimplementasikan. WIM dibuat dengan bahan *tamper proof* sehingga WIM dapat menggunakan PKI.

Pada saat ini belum ada telepon seluler yang telah mempunyai kemampuan WIM. Setidaknya Ericsson yang telah mengeluarkan model teleponnya pada tahun 2000 atau awal tahun 2001.

## **4.2 Penerapan dan Standar Pada Mobile Environment**

Penggunaan internet dengan menggunakan telepon seluler telah mulai berkembang beberapa tahun yang lalu. Model otentifikasi yang sekarang digunakan merupakan konsep yang diterapkan pada sistem dengan kabel(*wired*), tetapi ada beberapa konsep yang dikembangkan khusus untuk *mobile environment*.

### **4.2.1 Metoda Sedarhana**

Metoda otentifikasi yang digunakan pada masa lalu (*wire system*) juga digunakan pada *mobile system*. Pada service yang menggunakan WAP metoda yang umum digunakan pada otentifikasi adalah dengan menggunakan *username* dan *password*. Pada beberapa metoda otentifikasi juga berdasarkan pada nomor telepon selular seperti nomor MSISDN. Metoda otentifikasi ini sama dengan metoda yang digunakan pada komputer yang terhubung ke jaringan dengan menggunakan *IP-address*.

### **4.2.2 Produk yang ada Dipasar**

Ada beberapa vendor yang mengeluarkan produk yang dapat melakukan otentifikasi dan otorisasi pada *mobile environment*. Tetapi produk-produk ini menggunakan metoda otentifikasi dan otorisasi yang berbeda-beda sehingga tidak terstandar.

Pada masa depan mobile equipment manufaktur seperti Nokia, Ericsson dan Motorola akan melakukan standarisasi metoda otentifikasi dan otorisasi pada mobile environment, tetapi hasil dari pembahasan ini belum tersedia. MeT mengumumkan bahwa mereka akan bekerjasama dengan perancang standarisasi otentifikasi dan otorisasi yang ada sekarang dan akan melakukan arah perkembangan yang sama dengan yang telah dilakukan pada WAP forum dengan spesifikasi WTLS dan WIM[8].

#### **4.2.2.1 HST**

HST merupakan konsep PKI yang diterapkan di Finlandia. Ide dasarnya adalah setiap warga negara Finlandia mempunyai smartcard yang pada *smartcard* ini telah terdapat sertifikat dan *private key*. *Smartcard* ini digunakan sebagai alat otentifikasi jika warga negara akan berhubungan dengan pemerintah. Penerapan HST ini dengan menambahkan alat baca smartcard

dan software yang dapat mengakses data pada smartcard. Tetapi jika mekanisme ini diterapkan pada PKI maka tingkat keamanan sistem ini dipertanyakan.

#### **4.2.2.2 RSA Security – SecurID**

*RSA Security SecurID* merupakan sistem yang mengotentifikasi user dimana *Security Dinamic* sebagai vendornya. Produk ini bekerja berdasarkan kode PIN dan *authenticator* yang menghasilkan kode baru secara teratur berdasarkan interval waktu tertentu, dimana kode ini dapat digunakan oleh user sebagai *passcode*. Pada implementasi dilapangan yang memvalidasi *passcode* dan PIN dari *user* adalah *server*[10].

Sistem ini memberikan tingkat keamanan yang cukup tinggi, karena didasarkan pada dua faktor otentifikasi yaitu PIN dan *authenticator*. Kelemahan dari sistem ini adalah :

1. user dapat mendapatkan *authenticator* hanya pada *RSA Security* begitupun dengan *software* untuk servernya,
2. User harus selalu membawa peralatan tambahan yaitu *authenticator*,
3. Teknologi ini diperuntukkan pada jaringan dalam suatu perusahaan sebagai solusi otentifikasi.

#### **4.2.2.3 Sonera SmartTrust – SIM Security Client**

Sonera SmartTrust menawarkan solusi keamanan pada WAP. Produk dari sonera SmartTrust adalah SIM Security Client yang merupakan berdasarkan produk SIM toolkit, pada produk ini menerapkan konsep pada subbab 4.1.2. Bagian dari produk ini sesuai dengan software yang ada pada software yang disebut “*SmartTrust Security Server*” yang mengimplementasikan PKI [11, 9]

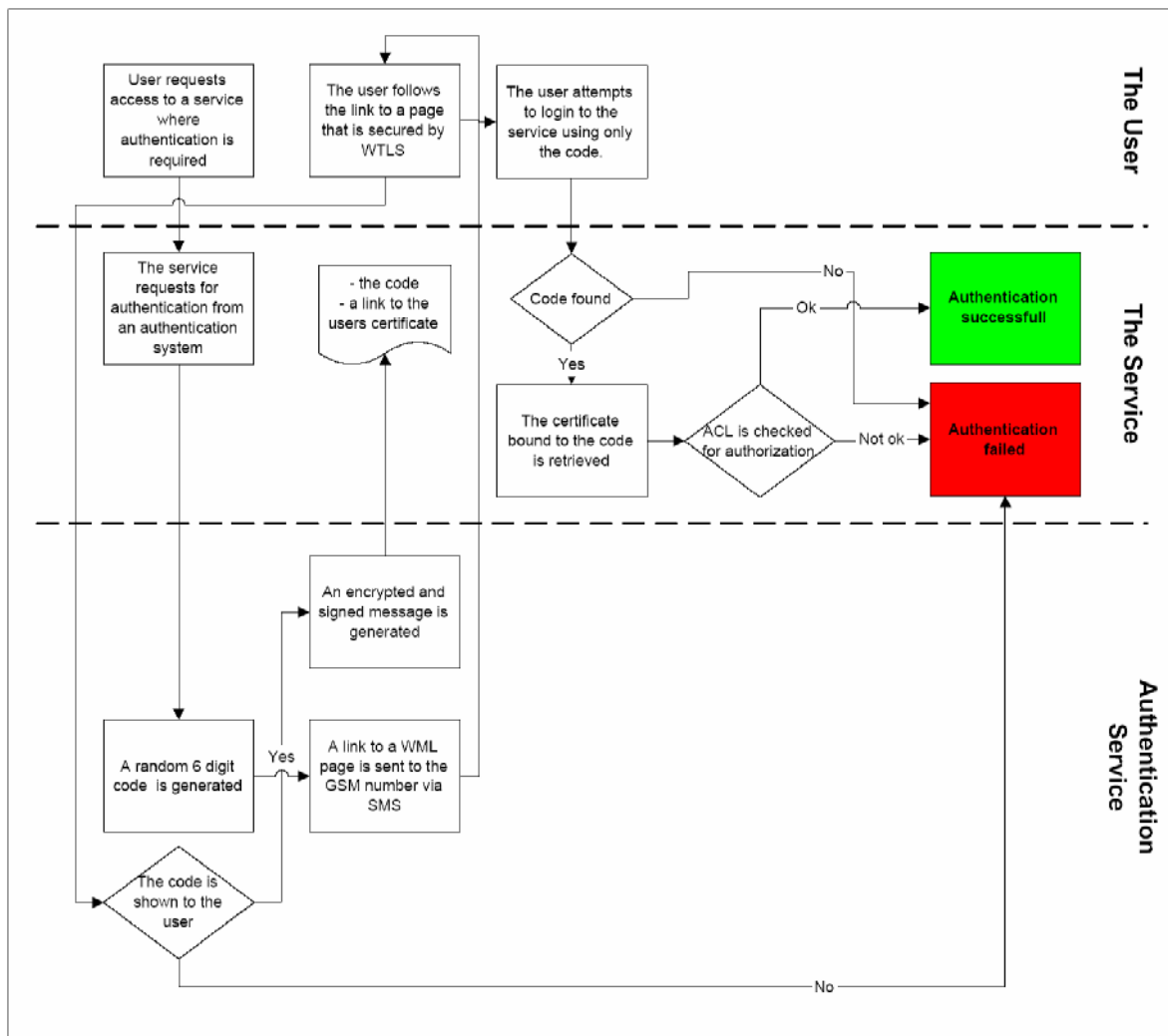
SmartTrust sangat baik diterapkan pada jaringan intranet, tetapi tidak pada jaringan yang lebih luas. Kelemahan dari produk ini adalah mengenai hak patennya. WIM pada dasarnya merupakan standar untuk mengimplementasikan fungsi-fungsinya dan tidak diragukan lagi sistem ini akan menjadi solusi pemecahan masalah dimasa depan.

### **4.3 Mekanisme Otentifikasi dan Otorisasi Secara Universal**

Pada bagian ini kemungkinan mekanisme otentifikasi dan otorisasi dapat dikombinasikan dengan akses kanal yang tersedia. Pada kenyataannya mekanisme ini belum terbukti dapat berjalan dengan baik sesuai dengan yang diinginkan, tetapi memungkinkan untuk diimplementasikan pada peralatan *mobile* yang mempunyai kemampuan sesuai dengan spesifikasi

pada [14, 13]. Mekanisme ini tentunya tidak diperlukan jika diakses melalui WAP, karena pada WAP telah ada WTLS handshake yang mengotentifikasi *user*.

Gambar dibawah ini merupakan ilustrasi dari mekanisme otentifikasi dan otorisasi, dimana pada mekanisme ini melibatkan tiga pihak yaitu *user*, *service* yang ingin diakses oleh user dan *authenticate service* yang merupakan tiga bagian yang terpisah. Pada mekanisme ini diasumsikan CA benar-benar ada dan dapat diakses melalui *network*.



Gambar : Flowchart yang menggambarkan mekanisme otentifikasi dan otorisasi

Adapun penjelasan dari flowchart diatas adalah :

1. *user* meminta hak akses kepada *services*, service ini dapat berupa *internet banking*. User dapat menggunakan internet (WWW) atau telepon sebagai kanal akses,
2. *service* meminta kepada *authenticate service* untuk mengotentifikasi user. Service melewatkan kepada *authenticate service* setidaknya hubungan (*link*) ke sertifikat dan nomor MSISDN *user*,

3. *authenticate service* membuat kode acak (panjang 6 digit) kode ini hanya berlaku dalam jangka waktu yang singkat (30-60 detik), karenanya kode ini tidak perlu terlalu panjang,
4. hubungan (*link*) terhubung ke halaman WML, dimana pada halaman ini terdapat kode yang akan dimasukkan ke MSISDN user. SMS (*Short Message System*), *OTA messages* atau *WAP push* dapat digunakan untuk melakukan hal ini. Halaman WML ini diamankan dengan *WTLS* sehingga otentifikasi user dibutuhkan pada *WTLS handshake*,
5. user mengikuti link ini. *WTLS handshake* secara otomatis melakukan otentifikasi dengan menggunakan fasilitas pada WIM,
6. *authentication service* memperhatikan apakah *WTLS handshake* berhasil atau tidak. Jika service yang diminta tidak merespon maka otentifikasi dianggap gagal dan jika berhasil maka service akan mengirim pesan yang berisikan minimal kode yang ditampilkan pada halaman WML dan link ke sertifikat user. Pesan ini dienkripsi dengan menggunakan *public key*, service mengirim sinyal kepada *authentication service* untuk bekerja dengan memberikan link ke sertifikat. Mekanisme ini merupakan mekanisme yang biasa dilakukan pada sertifikat X.509 atau sertifikat SPKI,
7. sekarang user dapat menggunakan service dengan hanya memasukkan kode yang telah diberikan,
8. ketika service menerima kode yang dimasukkan user, maka service akan melihat pesan (kode) yang terakhir dari *authentication service*, jika sama maka akan dicek identitas user dengan cara mengecek link ke sertifikat. Kemudian service mengecek ACL untuk mengetahui apakah user mempunyai otorisasi untuk mengakses service. Jika hasil pengecekan ACL ok maka user mempunyai otorisasi untuk mengakses service jika tidak maka otorisasi dianggap gagal.

**Keuntungan mekanisme ini adalah :**

1. aman – tingkat keamanan dapat disesuaikan dengan kebutuhan,
2. sederhana digunakan,
3. tahan terhadap serangan (*attacks*) – *life time* dan panjang kode menentukan tingkat keamanan,
4. mekanisme ini berdasarkan PKI (X.509), *WTLS* dan WIM yang merupakan metoda yang telah standar,
5. teori keanoniman dimungkinkan. Sistem otentifikasi dapat dilakukan dengan sertifikat SPKI tanpa harus menggunakan identitas *user*,
6. *user* hanya menggunakan telepon selular, dengan kemampuan *WTLS* yang dapat menjalankan *WAP browser* dan sertifikat WIM dengan *private key*,

7. metode otentifikasi yang sama dapat digunakan dengan melalui kanal yang berbeda,
8. user tidak harus mengingat password, selain dari PIN dari SIM/WIM.

**Kelemahan mekanisme ini adalah :**

1. sistem ini berdasarkan atas WAP yang *cumbersome* dengan koneksi data selular,
2. user harus membawa telepon selular ketika akan melakukan mengotentifikasi dirinya,
3. Usability belum tersedia.

## **BAB V**

### **KESIMPULAN**

Otorisasi misalnya dalam pembayaran merupakan masalah utama yang dihadapi jika akan melakukan e-commerce pada jaringan terbuka. Ditambah lagi jika service dan *resources* dapat diakses melalui jaringan informasi yang berbeda seperti jaringan mobile dan jaringan tetap (*fixed*) dan berbeda jenis alat dan *interface*.

PKI menyediakan dasar pada proses otentifikasi. Sertifikat X.509 merupakan standar yang telah digunakan pada lingkungan telepon GSM yang telah dilengkapi WAP *browser*. Manajemen kunci (*key*) merupakan permasalahan yang dihadapi dalam mekanisme ini. *Private key* yang sama seharusnya dapat digunakan dalam lingkungan yang berbeda baik pada *workstation* maupun pada telepon seluler.

WIM mungkin merupakan pemecahan dari masalah ini. Spesifikasi dari WIM baru berkembang dan akan terus dikembangkan oleh komunitas WAP standardization. MeT dibentuk oleh raksasa komunikasi dunia seperti Nokia, Ericsson, Motorola dan terakhir bergabung Siemens mencoba memecahkan masalah yang pada WAP forum dicoba untuk diatasi mengenai spesifikasi WTLS dan WIM.

Dengan teknologi sekarang ini, memungkinkan untuk menggunakan otentifikasi dan otorisasi yang didasarkan pada PKI dan dengan tingkat kegunaan yang tinggi. Hanya masa depan akan memperlihatkan model yang akan digunakan.

## Daftar Pustaka

- [1] Abelson, H. et al. The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption 20.8.1998, [referred 9.11.2000], <http://www.cdt.org/crypto/risks98/>
- [2] Branchaud, M. A Survey of Public Key Infrastructures March 1997, [referred 9.11.2000], <http://home.xcert.com/marcnarc/PKI/thesis/>
- [3] Diffie, W. and Hellman, M. New Directions in Cryptography, *IEEE Transactions on Information Theory* November 1976, pp. 644-654
- [4] Ellison, C. et al. RFC 2693 - SPKI Certificate Theory September 1999, [referred 9.11.2000], <ftp://ftp.ietf.org/rfc/rfc2693.txt>
- [5] Ford, M. Identity Authentication and 'E-Commerce' 30.10.1998, [referred 9.11.2000], <http://www.law.warwick.ac.uk/jilt/98-3/ford.html>
- [6] Gerk, E. Overview of Certification Systems: X.509, CA, PGP, and SKIP 17.4.1997, [referred 9.11.2000], <http://www.mcg.org.br/cert.htm>
- [7] Gerk, E. Towards Real World Models of Trust: Reliance on Received Information 23.1.1998, [referred 9.11.2000], <http://www.mcg.org.br/trustdef.htm>
- [8] The MeT Initiative. MeT Overview White Paper Version 1.0, 2 of October 2000, [referred 9.11.2000], <http://www.mobiletransaction.org/techinfo.html>
- [9] Puhakainen, P. Electronic Commerce: Market Estimates and Security Considerations Licentiate's thesis. Helsinki University of Technology. Espoo Finland. July 2000, [referred 9.11.2000], <http://www.certall.fi/finnish/content/businessarea/lic4.pdf>
- [10] RSA Security RSA SecurID, Web Portfolio. How RSA SecurID Agents Can Secure Your Website 2000, [referred 9.11.2000], [http://www.rsasecurity.com/products/securid/whitepapers/web/Web\\_Agent\\_Solution\\_WP.pdf](http://www.rsasecurity.com/products/securid/whitepapers/web/Web_Agent_Solution_WP.pdf)
- [11] Sonera SmartTrust Ltd. SmartTrust SIM Security Client 2000, [referred 9.11.2000], [http://www.smarttrust.com/products/sim\\_security\\_client.html](http://www.smarttrust.com/products/sim_security_client.html)
- [12] SSH Communications Security Introduction to cryptography 2000, [referred 9.11.2000], <http://www.ssh.com/tech/crypto/intro.html>
- [13] Wireless Application Forum, Ltd. Wireless Application Protocol, Identity Module Specification 18 February 2000, [referred 9.11.2000], <http://www.wapforum.org>
- [14] Wireless Application Forum, Ltd. Wireless Application Protocol, Wireless Transport Layer Security Specification 18 February 2000, [referred 9.11.2000], <http://www.wapforum.org>