FEDERATED DIGITAL IDENTITY MANAGEMENT DALAM MENDUKUNG *E-BUSINESS*

Ahmad Nurul Fajar
Dosen FASILKOM - UIEU
nurul.fajar@lecturer.indonusa.ac.id

Abstrak

Era digital yang telah merubah perilaku serta kebiasaan masyarakat dalam melakukan aktifitas telah dimanfaatkan oleh pihak yang tidak bertanggung jawab demi mendapatkan keuntungan dengan cara yang tidak legal. Kenyamanan dan rasa aman dalam melakukan aktifitas digital merupakan hal mendasar yang diharapkan oleh para penggunanya. Perkembangan bisnis yang demikian pesat telah menyebabkan terbentuknya kolaborasi diantara para pelaku bisnis dengan pemerintah. Pengaksesan informasi secara bersama sama telah terjadi dalam kolaborasi tersebut. *Digital identity* adalah suatu identitas yang digunakan untuk mengakses informasi secara digital. Paper ini coba memaparkan bagaimana *Identity Management* dari sudut pandang federasi (*federated identity), technology and architecture* dalam kaitannya dengan strategi pelaku bisnis

Kata Kunci: *Digital Identity, Digital Identity Management, Architecture, Federated Identity*

Pendahuluan

Identity dan *security*

Merupakan hal yang lazim dan sering terjadi penyalahgunaan *identity* dewasa ini. Pada dasarnya *identity* adalah autentikasi, otorisasi dan akses kontrol

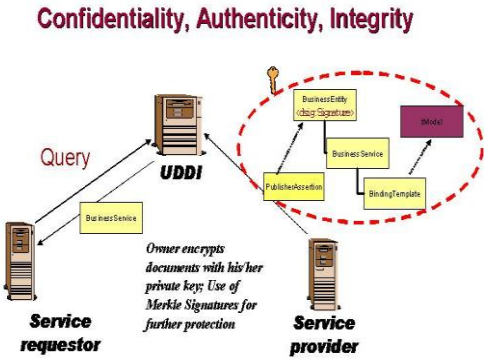
Identity dan Bisnis

Dewasa ini para pelaku bisnis telah memanfaatkan IT sebagai ujung tombak dan strategi perusahaan/organisasi mereka. Untuk beberapa pelaku bisnis di bidang penjualan telah menerapkan transaksi digital dalam menunjang proses bisnis mereka.

Digital Identity

Digital Identity adalah representasi dari identitas manusia yang digunakan pada jaringan terdistribusi antara manusia dan mesin. Tujan dari *Digital Identity* adalah untuk memberikan kemudahan dan keamanan bagi para pengguna saat melakukan transaksi. Representasi dari *Digital Identity* hanya diperlukan untuk melengkapi sebagian proses transaksi yang terjadi dan dapat dikatakan bahwa beberapa transaksi membutuhkan lebih dari satu identitas pengenal. Contoh yang paling sederhana dari *Digital Identity* terdiri dari ID *(user name)* dan autentikasi yang rahasia atau. *Password.* Pada pelaksanaanya *Digital Identity* menjadi sesuatu yang kompleks dan harus dikelola dengan baik dalam menentukan kevalidan dari tiap-tiap identitas. *Digital Identity* dapat meliputi beberapa hal di bawah ini antara lain:

- Autentikasi
  - Dalam sebuah transaksi elektronik, proses autentikasi dari identitas merupakan hal mutlak yang harus dilakukan oleh sistem. Autentikasi yang melibatkan banyak identitas dapat mengurangi dan meminimalisir terjadinya kejahatan transaksi.
- Akses kontrol
  - Proses berikutnya setelah autentikasi adalah mengenai akses kontrol, dimana dari masing masing Id memiliki akses kontrol yang berbeda – beda.
- *Confidentiality*
  - Kemampuan untuk mengetahui pihak-pihak mana saja yang memiliki otorisasi dan tidak. Hal ini dapat dilakukan dengan menggunakan enkripsi
- Data *integrity*
  - Untuk memastikan data tidak ada perubahan saat dilkaukan proses perpindahan data. Teknologi yang dikenal saat ini adalah PKI (*Public Key Infrastructure)*.
- *Control*



Sumber: www.oreillynet.com

Gambar 1. Keterkaitan beberapa *Digital Identity*

Tinjauan Teori

Identity

Apa yang dimaksud dengan *identity?* Menurut Salvador Minuchin, *Identity* memiliki dua elemen yaitu : siapa atau apa.

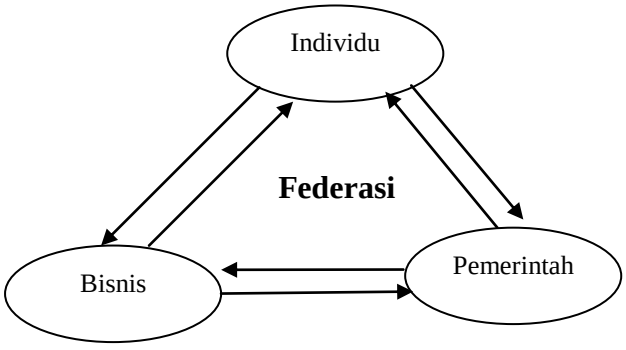
- *Who one is (identity)* yaitu menjelaskan siapa yang memiliki identitas/pengenal tersebut
- *The credentials that one holds (attributes of that identity)*, yaitu apa apa saja yang menjadi atribut dari identitas/pengenal tersebut

Menurut Tony Scott, *digital identity* adalah salah satu dasar dalam bagian pengembangan generasi IT masa depan.

Federated identity

Federated identity adalah kondisi dimana telah ada saling percaya dari masing masing organisasi/perusahaan yang terlibat, standarisasi yang sama, infrastruktur yang tersedia dan adanya kolaborasi *identity* yang sama untuk saling berbagi *identity,* proses bisnis.

Menurut Windley, Federated menggambarkan proses dan dukungan teknologi dimana satu *identity* dapat digunakan untuk mengakses banyak sumber daya informasi karena banyak variable *identity* telah di *mapping* menjadi global *identity*.



Sumber: www.burtoungroup.com

Gambar 2. *Federated Identity*

Reference Model

Model ini dikembangkan oleh Danish seorang IT-architects, berda-

sarkan dari Booz-Allen-Hamilton's model. *Reference Model* menjelaskan wilayah-wilayah yang ada dalam *Digital Identity Management*, yaitu:

- *Administration & management*
- *Credential issuing*
- *Storing*
- Autentikasi
- Autorisasi
- *Logging* dan *Control*

Dari area cakupan yang ada di dalam *Reference Model* masih belum adanya standarisasi yang baku pada masing masing cakupan. Untuk membuat standarisasi yang baku pada masing-masing cakupan diperlukan diskusi, penelitian dan eksplorasi bersama dari pihak-pihak yang berkolaborasi.

Reference Model juga belum mampu menjawab permasalahan *Federated Identity Management* yang merupakan kolaborasi individu, pemerintah serta pelaku bisnis. Penerapan *Federated Identity Management* di Indonesia yang belum optimal disebabkan beberapa aspek antara lain adalah:

- Rasa percaya
  - Penyalahgunaan teknologi oleh sebagian pihak telah menyebabkan adanya ketidakpercayaan atas teknologi. Untuk Menumbuhkan rasa percaya merupakan persoalan mendasar yang harus dilakukan secara bertahap dan dengan strategi yang baik
- Kultur/budaya
  - Budaya masyarakat Indonesia yang masih konvensional menyebabkan masih sulitnya teknologi baru masuk dan diterima ke dalam lingkungan system karena adanya beberapa pihak yang merasa kepentingannya akan diganggu dengan adanya teknologi
- Belum adanya IMA
  - Belum memiliki *Identity management architecture (IMA)*, sehingga tidak adanya master plan yang dijadikan sebagai acuan untuk melangkah dan bertindak.
- Birokrasi pemerintah
  - Prosedur yang terlalu birokratif menyebabkan sulitnya menerapkan konsep ini
- *Concern* pemerintah
  - Belum adanya kepedulian yang serius dari pemerintah untuk menerapkannya. Dukungan dan kepedulian yang serius sangat mutlak diperlukan.
- Infrastruktur dan sumber daya yang tersedia
  - Keterbatasan sumber daya dan infrastuktur sangat mempengaruhi keberhasilan dari kolaborasi yang dilakukan. Perbaikan infrastruktur dan pembenahan SDM harus dilakukan secara terencana.

Digital Identity management

Digital Identity management adalah sekumpulan proses yang aman untuk mendefinisikan, membuat, menangani dan memperbaharui informasi dasar dari para individu. Beberapa teknologi yang digunakan untuk *Digital Identity management* adalah data *mining, ontology management* dan *federated computing.*

Pembahasan

Kolaborasi dari berbagai organisasi/perusahaan menyebabkan adanya *resource* yang dapat digunakan bersama-sama. Untuk dapat mengimplementasikannya diperlukan beberapa hal antara lain adalah:

- Keamanan (*Security)*
  - Masalah keamanan merupakan masalah penting dalam suatu aplikasi komputer dan jaringan komputer. Dengan adanya *resource* yang dapat digunakan bersama mengakibatkan banyak sekali user/pengguna yang memiliki peluang dan potensi untuk melakukan tindakan yang merugikan.
- Kepercayaan *(trust)*
  - Saling percaya antara masing-masing perusahaan yang berkolaborasi mutlak diperlukan.
- Standarisasi autentikasi
  - Autentikasi yang dilakukan harus memiliki standar yang baku bagi pihak yang berkolaborasi
- Standarisasi autorisasi
  - Autorisasi yang dilakukan harus memiliki standar yang baku bagi pihak yang berkolaborasi
- Pertukaran informasi secara terbuka
  - Dengan adanya kolaborasi dan penggunaan *resource* bersama menyebabkan pertukaran informasi bebas dan terbuka untuk pengguna
- Perlindungan informasi privat
  - Harus adanya perlindungan dan jaminan bahwa informasi yang sifatnya privat atau rahasia harus dilindungi.

Identity Management Architecture (IMA)

Identity Management Architecture dapat dianalogikan seperti "perencanaan kota". Pada masing masing kota, kita dapat melihat situasi dimana adanya kesenjangan dan kesemrawutan tata letak kota tersebut. Kebijakan dan aturan standar dalam pengelolaan kota dan pengaturan warga kota tersebut juga banyak yang tidak konsisten. Perencanaan kota yang baik haruslah memikirkan pembuatan standarisasi kebijakan dan aturan yang nantinya akan menciptakan sinergi antara kehidupan masyarakat, lingkungan, bangunan/infrastruktur. IMA merupakan sekumpulan kebijakan dan aturan yang standar untuk memberikan cakupan dalam membuat identitas digital yang tangguh dan handal

Phase-Phase IMA

Ada beberapa phase dalam IMA:

- Inisiasi
- Pembangunan
- Implementasi

Keuntungan *Identity management architecture (IMA)*

Identity management architecture (IMA) banyak memberikan keuntungan bagi pengguna dan pelaku bisnis. Perbedaan dengan konsep keamanan tradisional adalah di dalam IMA tidak hanya sekedar menggunakan konsep "bagaimana cara menjaga daan melindungi" tetapi lebih komprehensif dengan adanya sinergi serta keterkaitan antara beberapa aspek. IMA memberikan master plan (*blue print*) mengenai bagaiman cara mengelola aset informasi, karena informasi tersebut dapat dikategorikan sebagai aset.

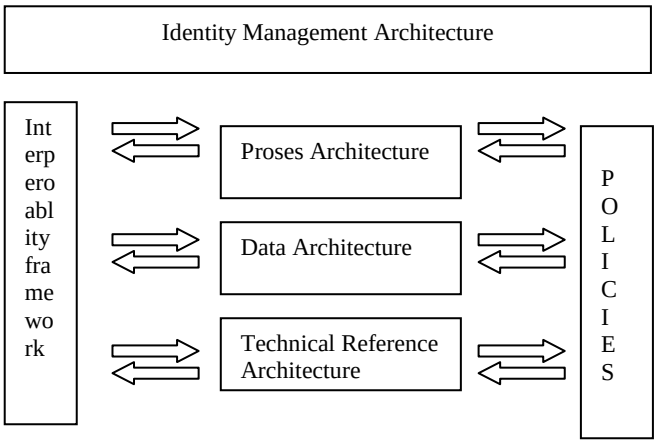
Faktor Keberhasilan *Identity Management Architecture (IMA)*

Ada beberapa faktor yang menjadi kunci keberhasilan IMA:

- Pihak eksekutif peduli dan concern terhadap kebutuhan *Identity management*
- Komitmen dari resource yang ada
- Sumber daya IT di organisasi tersebut
- Kultur atau budaya di organisasi

Komponen *Identity Management Architecture (IMA)*

Dalam membangun IMA meliputi keterkaitan antara beberapa komponen. Hal ini disebabkan IMA tidak hanya berbicara tentang satu persoalan/komponen yang terpisah dengan komponen yang lain.



Governance Framework and Business Context

Sumber: www.oreillynet.com

Gambar 3. Komponen IMA

Data Architecture adalah model data identitas dalam suatu organisasi yang meliputi tiga area yaitu :

- Pengkategorian
- Perubahan dan
- Struktur data

Identity Policies adalah cara organisasi untuk membawa arah kebijakan organisasi dan menciptakan lingkungan system. Kebijakan atau policies yang diciptakan harus sesuai dengan visi organisasi sehingga nantinya arah kebijakannya tersebut akan sejalan

Technical Reference Architecture memberikan tuntunan implementasi untuk arsitek sistem bagaimana merancang sistem yang saling berinteraksi satu sama lain berdasarkan *identity infrastructure.*

Kesimpulan

Federated Digital Identity Management merupakan hal fundamental bagi para pelaku bisnis, individu dan pemerintah yang ingin menerapkan proses bisnis secara digital. Dengan adanya kolaborasi menyebabkan penggunaan resource secara bersama-sama menyebabkan security menjadi persoalan utama. Persoalan security tidak hanya konvensional dengan sekedar melindungi ataupun menjaga, tetapi melibatkan banyak komponen yang saling bersinergi secara komprehensif. Untuk mendapatkan hasil yang optimal diperlukan pembangunan IMA *(Identity Management Architecture)* dengan memperhatikan keterkaitan dari masing-masing komponen.

Daftar Pustaka

Amir Hadziahmetovic, Master Thesis IT University Of Copenhagen

Abhilasha Bhargav-Spantzel Anna C. Squicciarini Elisa Bertino

CERIAS and Department of Computer Science, Purdue University "Integrating Federated Digital Identity Management and Trust Negotiation– issues and solutions "

E. Bertino, E. Ferrari, and A. C. Squicciarini. Trust-_: A Peer-to-Peer Framework for Trust Establishment. *IEEE Transactions on Knowledge and Data Engineering*, 16(7):827– 842, July 2004.

Elisa Bertino, Abhilasha Bhargav-Spantzel, Anna Cinzia Squicciarini CERIAS and Computer Science Department Purdue University West Lafayette, IN "Policy Languages for Digital Identity Management in Federation Systems"

http://www.burtongroup.com/coverage_areas/federated/research.asp

http://www.oreillynet.com/pub/a/network/2005/08/19/digitaldentity.html

http://www.oreillynet.com/pub/a/network/2005/08/19/digitaldentity.html?page=2

http://www.windley.com/archives/2004

http://www.windley.com/archives/2004/01/identity_manage_2.shtml

http://conference.digitalidworld.com/2004/attendees/slides/1026_1100_C.pdf

Morten Storm Petersen's slides from the IT-security conference 2006, held on 18. January 2006.