Doc Name	Pilar E-Gov : Data Interchange Framework (Focus : Security)
Reference	Apkomindo, IT-Corner Tribun Kaltim
Date	May, 2004
Status	***DRAFT – PUBLIC READABLE***
Version	1a
Author	Anton Rahmadi, S.Tp – Konsultan TI
Editor	

Penggunaan Teknologi Informasi;
E-Government : Framework Publik, Terbatas, dan Privat

Oleh Anton Rahmadi
Konsultan TI

Menyambung tulisan minggu lalu, setelah membahas mengenai *Political Encourage* dan *Human Resources*, faktor suksesnya E-Government berikutnya adalah Konsep Umum Keamanan (*Security Framework*). Sudah sering dibahas, faktor ini juga merupakan titik lemah pengembangan TI di kalangan pemerintahan. Secara garis besar, saat ini, pengembangan TI di kalangan pemerintahan masih terfokus pada pengadaan dan website. Anehnya, dari tahun ke tahun, tampaknya proyek-proyek masih saja berkutat di bidang tersebut, tanpa ada *planning* yang jelas ke depan dalam bentuk *framework*.

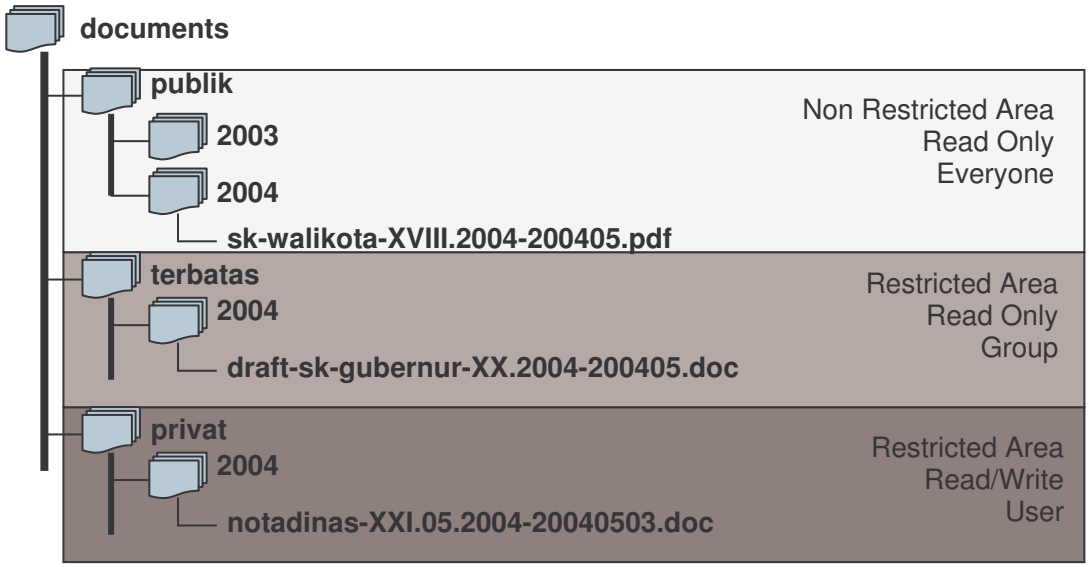
Bermigrasi dari kerja menggunakan kertas, sebagian instansi sudah memulai untuk bekerja menggunakan dokumen digital, atau file-file di dalam komputer. Langkah selanjutnya yang merupakan tren adalah membangun jaringan intranet dan internet, dimana hampir semua instansi pemerintahan memiliki website. Namun sayangnya data-data yang ditayangkan cenderung tidak diurus, apalagi sampai berbicara mengenai konsep penyimpanan data digital yang aman. Menyentuh masalah prosedur standar operasional saja belum, apalagi *concern* pada masalah *security*. Padahal, menggunakan internet dan intranet, memungkinkan pengguna untuk bekerja secara bersama (*collaboration*). Contoh yang paling mudah dalam kerja bersama ini adalah adanya publikasi dan pertukaran data digital yang memiliki keunggulan cepat, murah, dan akurat.

Konsep umum dalam publikasi maupun pertukaran data adalah keamaanan dan kerahasiaan sesuai keperluan. Bila digabungkan dengan teknologi website, yang memungkinkan terciptanya sistematika kerja yang lebih efisien dengan menganut konsep *anytime-anywhere*, keamanan dan kerahasiaan data ini menjadi sangat penting untuk

diketahui baik di tingkat operator, mid-manager (kabid/karo/kasi/kabag), dan eksekutif di pemerintahan. Sebagai contoh, tentunya akan menjadi berita "panas" bila muncul dokumen draft mutasi ditingkat publik, sementara status data yang seharusnya adalah privat (sangat rahasia) bagi *top level executive* (gubernur, walikota, atau bupati misalnya).

Secara krusial, pemerintahan memiliki sedikitnya tiga jenis keamanan dalam data, yang pertama adalah **publik**, dimana akses terhadap data tidak dibatasi kepada publik. Peran pers dan humas adalah menyebar luaskan informasi yang bersifat publik ini. Tolok ukurnya adalah makin mengertinya masyarakat akan suatu informasi, maka sosialisasi dianggap semakin sukses. Dokumen yang termasuk dalam data publik adalah rancangan peraturan daerah, peraturan daerah, pengumuman serta beberapa jenis surat keputusan, surat pemberitahuan, dan surat edaran. Dokumen-dokumen terklasifikasi publik ini sebaiknya ditampilkan dalam website milik pemerintahan mengacu pada instansi setempat dan terarsip dengan rapi misalkan berdasarkan tahun, bulan, dan instansi yang mengesahkan. Contoh penamaan dokumen publik yang baik misalnya : sk-walikota-XVIII.2004-200405.pdf yang disimpan dalam folder publik tahun 2004 (lihat Gambar 1.). Format dokumen juga disusun dalam format final yang tidak dimungkinkan terjadi perubahan, seperti PDF, ataupun HTML biasa, dan bukan file dokumen dalam format office (DOC,XLS, atau PPT).

Selanjutnya, klasifikasi dokumen yang kedua adalah **terbatas**. Dari penamaannya, dokumen ini jelas bukan merupakan konsumsi publik. Hak akses publik dibatasi (*restricted area*) dengan *password* yang hanya dipegang oleh orang-orang tertentu, sesuai kapasitasnya. Contoh saja draft dokumen SK gubernur yang belum ditandatangani, hanya menjadi konsumsi kalangan DPRD, Sekretaris Daerah, dan Asisten III misalnya. Format dokumen boleh saja menggunakan format "mentah" seperti DOC, sehingga masih dapat diubah oleh orang-orang terpilih (dalam istilah komputer *group users*). Penulisan sk juga dilakukan secara sistematis, sehingga memudahkan dalam pencarian arsip kembali. Sekali lagi, contohnya : draft-sk-gubernur-XX.2004-200405.doc (Gambar 1).



Gambar 1. Contoh penyimpanan data berdasarkan kerahasiaan dan data

Perlu dijelaskan, aplikasi yang digunakan sekali lagi berbasis website, dan inilah sebenarnya fungsi dari sistem informasi manajemen (SIM), bukan sekedar menampilkan data-data final, tapi dapat juga digunakan sebagai media kerja dengan asas *anywhere-anytime*.

Sebagai bagian yang terakhir, tentu saja perlu klasifikasi dokumen **privat**, dimana hanya sang pemilik ataupun user tujuan yang dapat membuka file dimaksud. Contohnya nota dinas, selain pejabat dimaksud, pengguna lain tidak diperbolehkan mengakses data tersebut, apalagi sampai tersebar ke publik. Sebagai contoh, penggunaan nota dinas atau memo secara *online* sudah mulai diujicobakan di lingkungan Kantor Ketenagakerjaan Balikpapan. Contoh lain, adalah *self-assesment* pegawai lingkungan pemprop Kaltim yang ujicobanya telah dapat diakses melalui situs http://www.bkd-kaltim.go.id.

Enkripsi dan Secure Socket Layer

Bagian lain teknik untuk meningkatkan keamanan data adalah melakukan pengacakan (*encrypting*) data. Dimana pada proses enkripsi ini, user diminta memasukkan kata kunci pengacakan yang harus diketahui oleh pengguna yang ingin membuka file dimaksud. Cara kerja enkripsi adalah mengacak data dalam format biner kemudian menukar karakter biner berdasarkan metode tertentu dan kata kunci yang

dimasukkan oleh user. Hasil dari pengacakan ini, dokumen tidak akan terbaca langsung, tetapi harus melalui proses deskripsi yang meminta kata kunci tersebut. Teknik ini dapat dipadukan dengan layanan SMS. Setelah data dienkripsi dan dikirim pada folder "terbatas", user dimaksud baru dapat mengakses setelah mendapatkan password dari SMS pemilik data. Cara ini relatif aman, namun masih dapat ditembus dengan metode *sosial engineering*, dimana seorang pejabat yang kurang memahami proses dekripsi, meminta kepada anak buahnya dan memberikan passwordnya. Hasilnya informasi tidak lagi bersifat rahasia.

Teknik terakhir yang dibahas kali ini adalah menggunakan jalur layanan khusus yang disebut *Secure Socket Layer* (SSL). Prosess ini memungkinkan terjadinya enkripsi dan dekripsi otomatis dalam sebuah lapisan layanan website untuk memastikan tidak adanya gangguan pencurian data ditengah jalan.

Jika semua metode ini digabungkan, yang perlu dipikirkan oleh pihak pengembang, tentunya bagaimana menciptakan aplikasi yang aman, namun mudah untuk digunakan dan tidak bermasalah saat diimplemantasikan, apalagi mengingat sifat umum dari bangsa kita yang tidak mau "repot" dan tidak "sempat" menambah ilmu.