

# PERANCANGAN SISTEM INFORMASI SIGNATURE VERIFICATION SYSTEM FOR BANKING

**Ikrar Adinata Arin**

Information System Departement, School of Information System  
Jl. K. H. Syahdan No. 9, Palmerah, Jakarta Barat 11480  
ikrar@binus.ac.id

## ABSTRACT

*Every teller of Bank XYZ Teller needs to verify and validate the customer's signature for withdrawal transactions done at the bank in order to avoid manipulation of original signature of the customer. If the amount of withdrawals money made is very large number (typically for corporate customers), the risk of manipulation becomes higher. Therefore, there is a need to implement a kind of software applications which functions as a tool to verify the signatures of banking customers. The author conducted a Signature Verification System for business operational of Bank XYZ.*

**Keywords:** application, verification, signature, banking customer

## ABSTRAK

*Salah satu kendala yang sedang dialami oleh masing-masing Teller Bank XYZ ketika melayani transaksi penarikan uang nasabah di masing-masing kantor adalah melakukan verifikasi dan validasi tanda tangan nasabah, apakah cocok dengan "original signature" nasabah tersebut, demi menghindari penyalahgunaan tanda tangan si pemilik rekening. Jika jumlah penarikan uang yang dilakukan oleh nasabah dalam jumlah yang sangat besar (biasanya untuk nasabah corporate), resiko penyalahgunaan tanda tangan tersebut sangat besar. Dibutuhkan suatu implementasi teknologi informasi berupa aplikasi software yang dapat melakukan fungsi sebagai alat untuk memverifikasi tanda tangan nasabah yang melakukan transaksi perbankan. Penulis melakukan perancangan sistem informasi banking signature verification system untuk kebutuhan operasional bisnis Bank XYZ.*

**Kata kunci:** aplikasi, verifikasi, tanda tangan, nasabah bank

## PENDAHULUAN

Sistem verifikasi (otentikasi) merupakan salah satu bentuk sistem keamanan yang digunakan untuk mengenali identitas seseorang dan menentukan apakah ia berhak atau tidak atas sumber daya tertentu. (Deviani, 2004). Saat ini Bank XYZ dan beberapa kantor cabangnya yang tersebar di beberapa kota di Indonesia, masih melalui proses yang cukup rumit dan kompleks dalam melayani kegiatan transaksi yang dilakukan oleh nasabahnya. Terbatasnya jumlah unit mesin penarikan uang otomatis (ATM) yang dimiliki oleh Bank XYZ, mengharuskan setiap nasabah yang ingin melakukan transaksi penarikan uang harus secara langsung mendatangi kantor cabang Bank XYZ terdekat.

Salah satu kendala yang sedang dialami oleh masing-masing *Teller* Bank XYZ ketika melayani transaksi penarikan uang nasabah di masing-masing kantor adalah melakukan verifikasi dan validasi tanda tangan nasabah, apakah cocok dengan "*original signature*" nasabah tersebut demi menghindari penyalahgunaan tanda tangan si penarik uang. Jika jumlah penarikan uang yang dilakukan oleh nasabah dalam jumlah yang sangat besar (biasanya untuk nasabah *corporate*), penyalahgunaan tanda tangan tersebut sangat besar resikonya jika benar-benar terjadi.

Belum adanya integrasi antar kantor cabang Bank XYZ untuk proses pencocokan tanda tangan, seorang *Teller* kantor cabang yang melayani nasabah yang melakukan penarikan uang diharuskan mengirimkan sampel tanda tangan via fax ke kantor Bank XYZ lain yang memiliki "*speciment signature*" nasabah tersebut. Dan ketika selesai di cek dan dicocokkan baru kemudian transaksi penarikan tersebut bisa dilakukan. Untuk menyederhanakan proses yang telah diceritakan di atas, dikembangkan sebuah sistem verifikasi tanda tangan yang nantinya dapat dilakukan secara cepat dan *online* oleh masing-masing *Teller* Bank XYZ.

## METODE

Metode perancangan sistem melalui beberapa tahapan, yaitu analisis, perancangan dan pembuatan sistem, pengujian, serta evaluasi hasil pengujian. Analisis dilakukan dengan menggali informasi mengenai karakteristik dan metode sistem verifikasi tanda tangan. Perancangan sistem dilakukan dengan model *prototyping*. Pengujian dilakukan dengan mengumpulkan spesimen Kartu Contoh Tanda Tangan (KCT) nasabah Bank XYZ yang telah di scan. Kemudian data KCT akan di-*upload* atau disimpan di dalam sebuah *server database* yang terletak di kantor pusat. Sistem verifikasi tanda tangan akan dibuat secara *online* di mana masing-masing user (*Teller*) yang berada di masing-masing Kantor Cabang terhubung dalam jaringan LAN/WAN dengan *server Database* yang berada di Kantor Pusat. Perangkat *Teller* aplikasi berupa PC yang sudah di-*install client* aplikasi akan mengakses data kartu contoh tanda tangan (KCT) di *server* tersebut. Dengan menggunakan metode ini, sistem dapat menerima input jumlah KCT yang di-*scan* dalam jumlah banyak dan menampilkannya secara bersamaan di perangkat *Teller*.

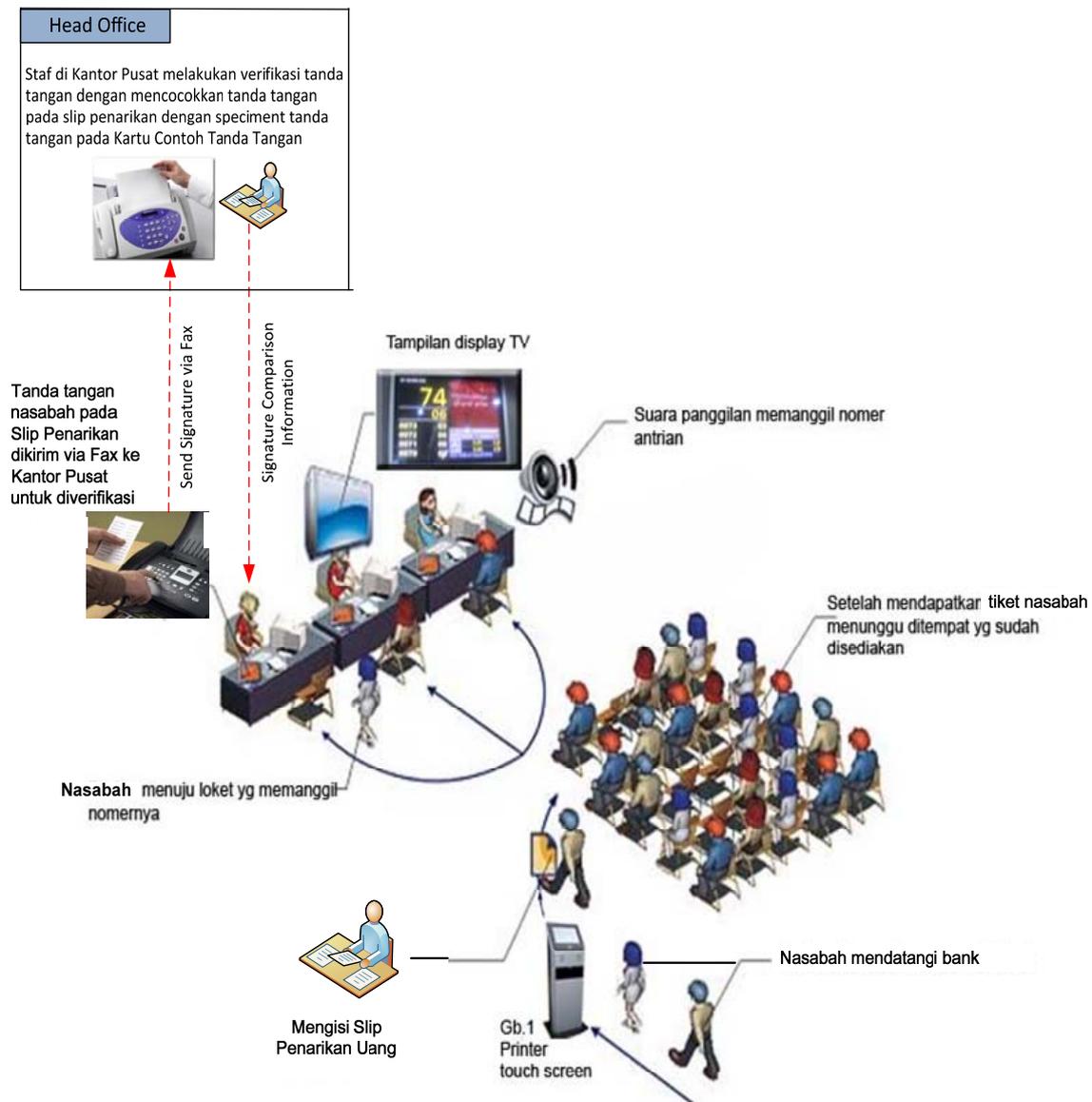
## HASIL DAN PEMBAHASAN

### Sistem Verifikasi yang Sedang Berjalan

Metode pengecekan tanda tangan yang saat ini diterapkan dan dijalankan oleh Bank XYZ masih bersifat manual dan membutuhkan waktu yang lama untuk sekali proses pengecekan tanda tangan. Pengecekan tanda tangan yang sesuai dengan data rekening nasabah khususnya yang

melakukan transaksi perbankan seperti penarikan uang akan dilakukan untuk menghindari penyalahgunaan wewenang.

Berikut gambaran atau ilustrasi proses penarikan uang milik nasabah yang harus melakukan proses verifikasi tanda tangan secara manual terlebih dahulu (proses sekarang), di mana *Teller* harus mencocokkan tanda tangan nasabah yang tertera pada slip penarikan dengan mengirimkan melalui faksimili ke kantor pusat (Gambar 1).

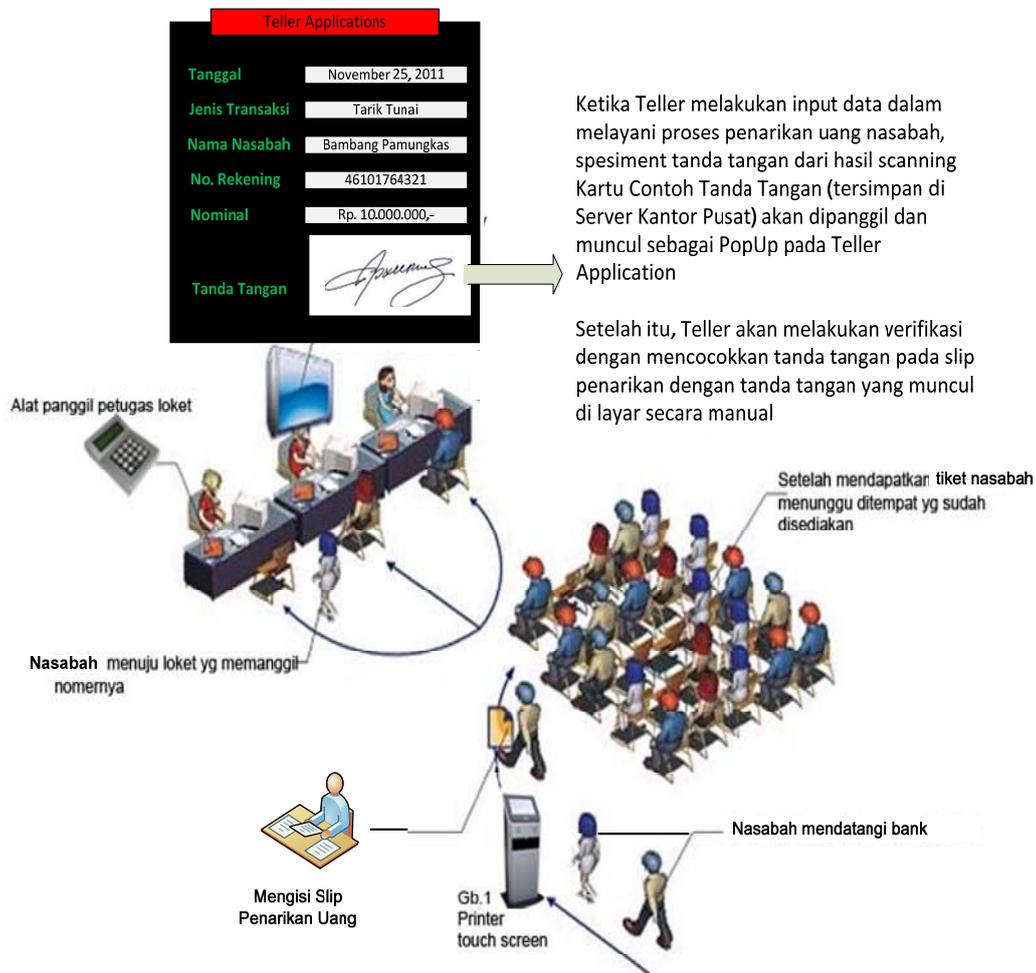


Gambar 1 Prosedur pengecekan tanda tangan sistem lama

## Sistem Verifikasi yang Diusulkan

Proses verifikasi yang baru lebih mudah, di mana *Teller* hanya tinggal memasukkan nomor rekening nasabah melalui client aplikasi, dan nantinya pada layar monitor akan ditampilkan KCT nasabah tersebut yang sudah tersimpan pada *server* Database di Kantor Pusat. *Teller* hanya tinggal

memasukkan nomor account (rekening) pada minor aplikasi klien yang terpasang pada *workstation* masing-masing, di mana sistem SVS secara otomatis mengambil *specimen* tanda tangan di *server* database KCT setiap kantor cabang. Pengecekan tanda tangan pada slip transaksi nasabah (slip penarikan, giro, cek dll) dengan mencocokkan tanda tangan yang tampil di layar monitor *Teller* (Gambar 2).



Gambar 2 Prosedur pengecekan tanda tangan sistem baru

## Scopes and Limitations

Aplikasi SVS dikembangkan berbasis *Client Server*, di mana pada masing-masing *workstation* pengguna akan diinstal dengan sebuah minor aplikasi klien untuk dapat menggunakan aplikasi SVS. Sedangkan main aplikasi akan diinstal pada *Server* yang ada di Kantor Pusat.

## User Capability

Secara fungsi aplikasi SVS ini adalah aplikasi berbasis *Client Server*, di mana aplikasi-aplikasi yang berhadapan dengan pengguna dapat melakukan fungsi-fungsi sebagai berikut: (1) *maker*, yaitu pengguna yang bertugas melakukan input data KCT (kartu contoh tangan) nasabah (*Customer*

*Service*). Data yang di-input masih berupa *temporary data*; (2) *checker*, yaitu pengguna yang bertugas melakukan proses *approval*/pengesahan KCT yang telah di-*input* oleh CS menggunakan aplikasi SVS. Data ini sudah berupa *fix data* dan bisa digunakan seutuhnya untuk proses verifikasi tanda tangan oleh *teller*; (3) *teller*, yaitu pengguna yang bertugas melakukan proses verifikasi tanda tangan, dengan membanding tanda tangan pada slip transaksi dengan tanda tangan yang muncul pada layar monitor.

## Software Development

Aplikasi SVS dikembangkan dan dibangun di atas *Operating System* yang terinstal pada perangkat sehingga tidak akan terjadi tumpang tindih *resources* dan fungsi bagian dari OS dengan beberapa aplikasi lain yang berjalan

### Server Application

Ini adalah aplikasi SVS yang akan diinstal pada perangkat *server* di Kantor Pusat Bank Victoria. Aplikasi ini berfungsi sebagai aplikasi yang dapat melakukan proses collect data KCT yang sudah discan di kantor pusat, dikirimkan dan disimpan di *server*. Kemudian dapat melakukan proses searching data KCT dan mengirimkan kembali ke pengguna yang membutuhkan contoh tanda tangan untuk proses verifikasi transaksi. *Server application* dibangun dengan menggunakan bahasa pemrograman Java.

### Client Application

Ini adalah aplikasi SVS yang akan diinstal pada masing-masing *workstation* pengguna. Aplikasi ini berfungsi sebagai aplikasi untuk proses scanning/creating data KCT dan mengirimkan data tersebut ke *server* di Kantor Pusat. Untuk tanda tangan KCT yang tersimpan pada *server* Kantor Pusat dan di-retrieve akan ditampilkan pada layar monitor *Teller* sebagai “pop-up”. *Client Application* dibangun dengan bahasa pemrograman Java /.NET

## Network Configuration

Aplikasi SVS dibangun secara *centralized*, dalam arti aplikasi utama akan diinstal pada *Server* KCT di Kantor Pusat, dan kantor cabang/kas yang memiliki *workstation* yang sudah terinstal *client application* dapat mengakses data KCT tersebut. *Network configuration* dapat dilihat pada Gambar 3.

## Behavioral Requirements

*Use Case SVS System* adalah sebagai berikut (Gambar 4). Selanjutnya, di bawah ini adalah *Activity Diagram SVS System* (Gambar 5 – 8).

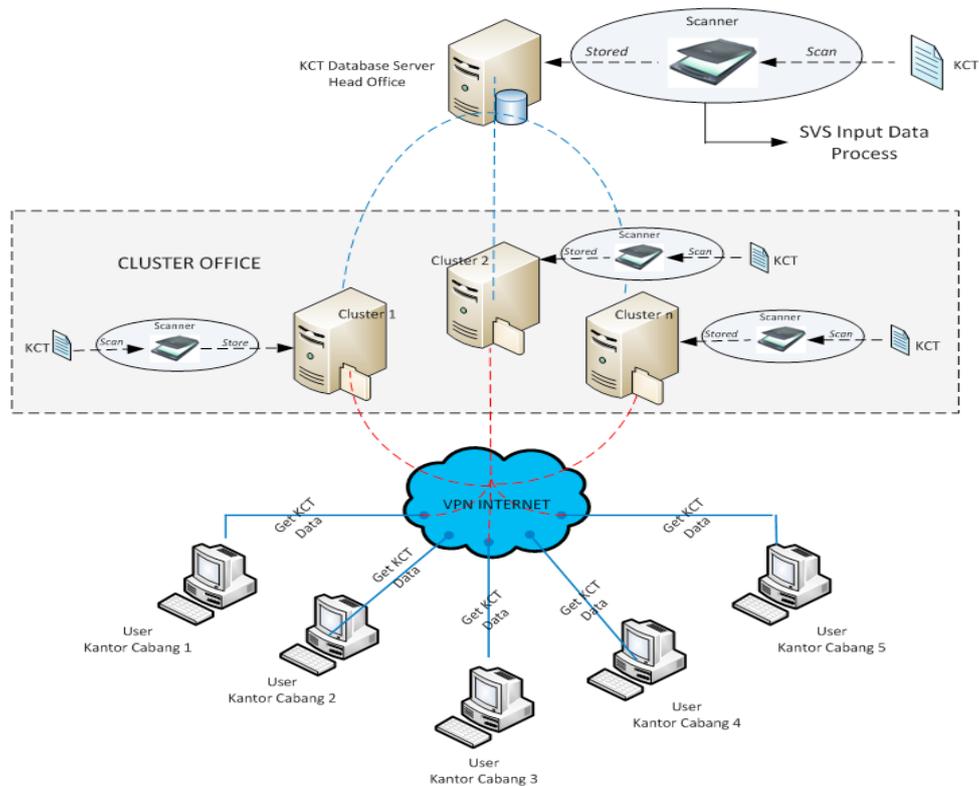
## Hardware Interfaces

Aplikasi SVS hanya dapat diakses melalui *workstation* pengguna berupa PC Dekstop atau Notebook sudah terpasang *Client Application*. Konfigurasi IP Address *workstation* dengan IP Address *Server* SVS pada Kantor Pusat harus dapat terkoneksi.

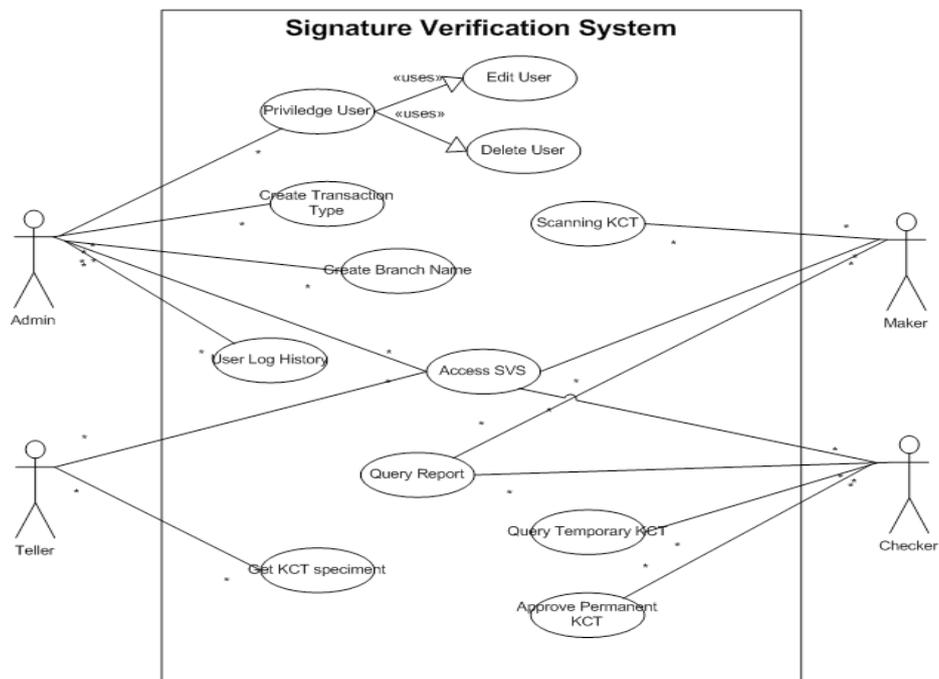
## Software Interfaces

Aplikasi SVS berinteraksi dengan aplikasi CoreBanking Bank Victoria, di mana nantinya ketika si pengguna (*Teller*) memasukkan nomor rekening nasabah ketika menggunakan aplikasi

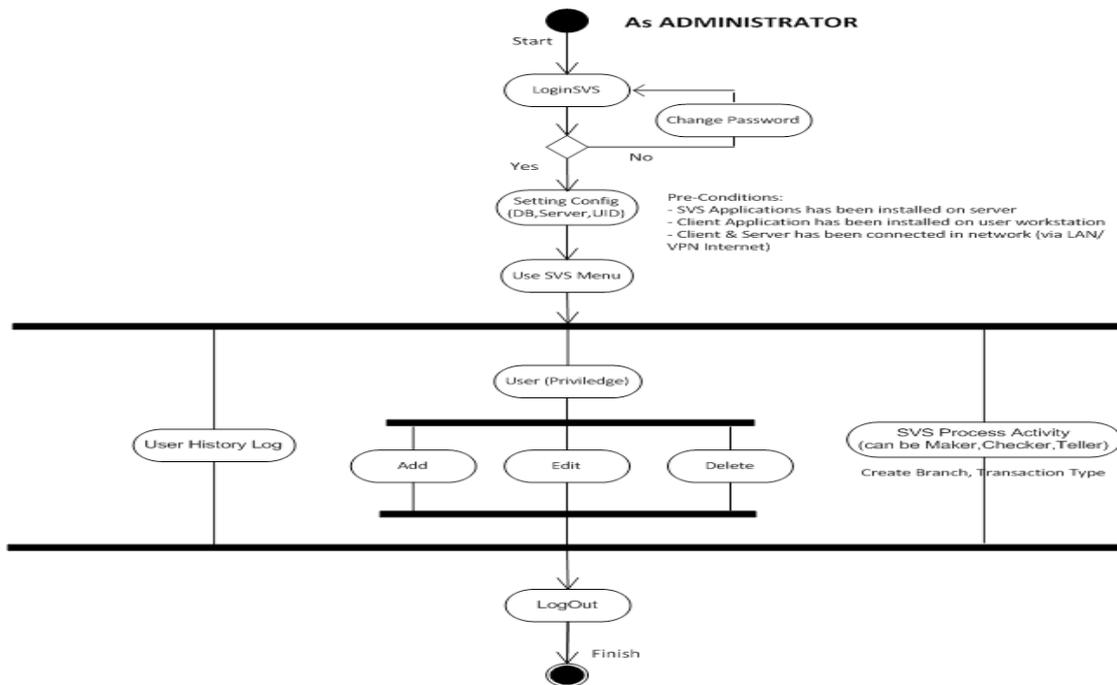
AlphaBits, si *Teller* akan ditampilkan pada layar monitornya *file* hasil scanning KCT yang di retrieve dari *server* di Kantor Pusat.



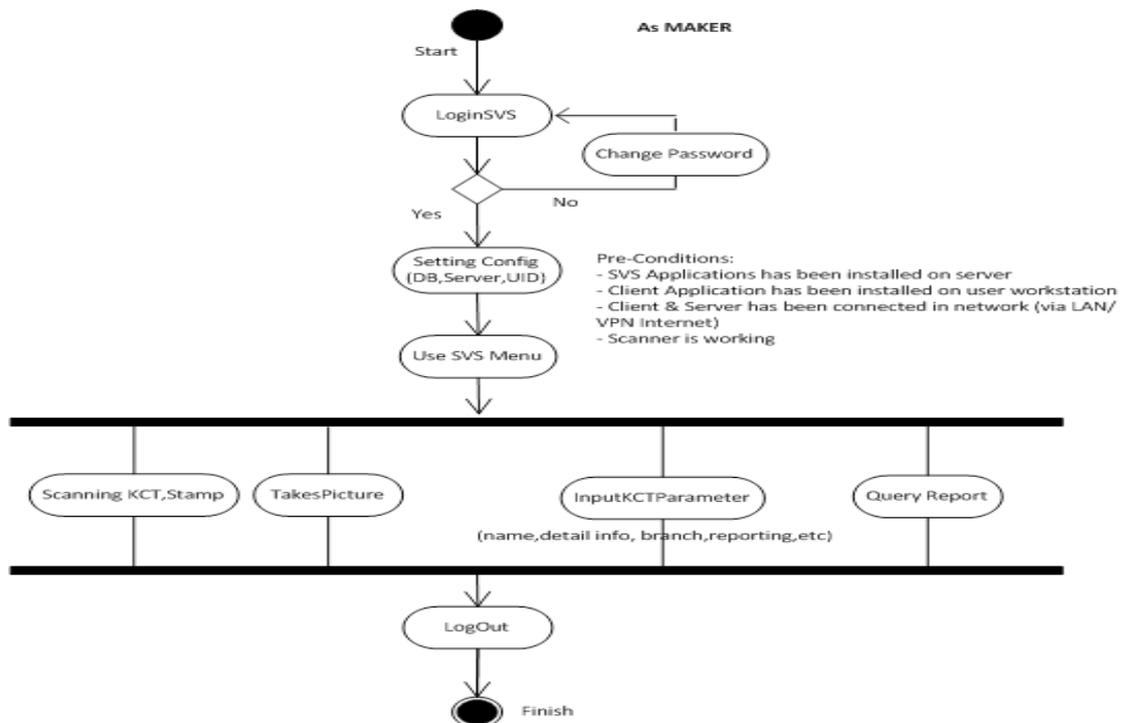
Gambar 3 Network configuration



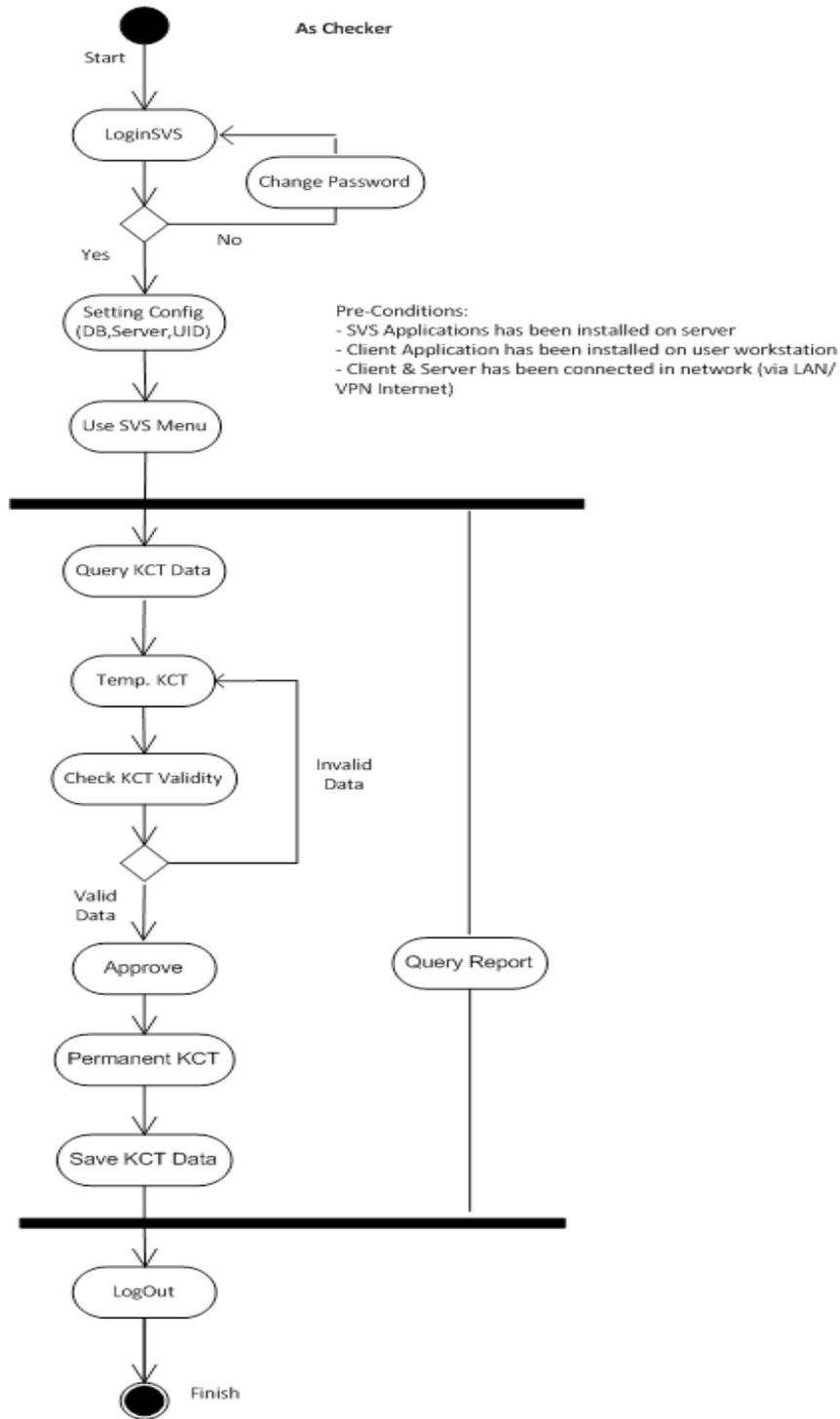
Gambar 4 Use case SVS system



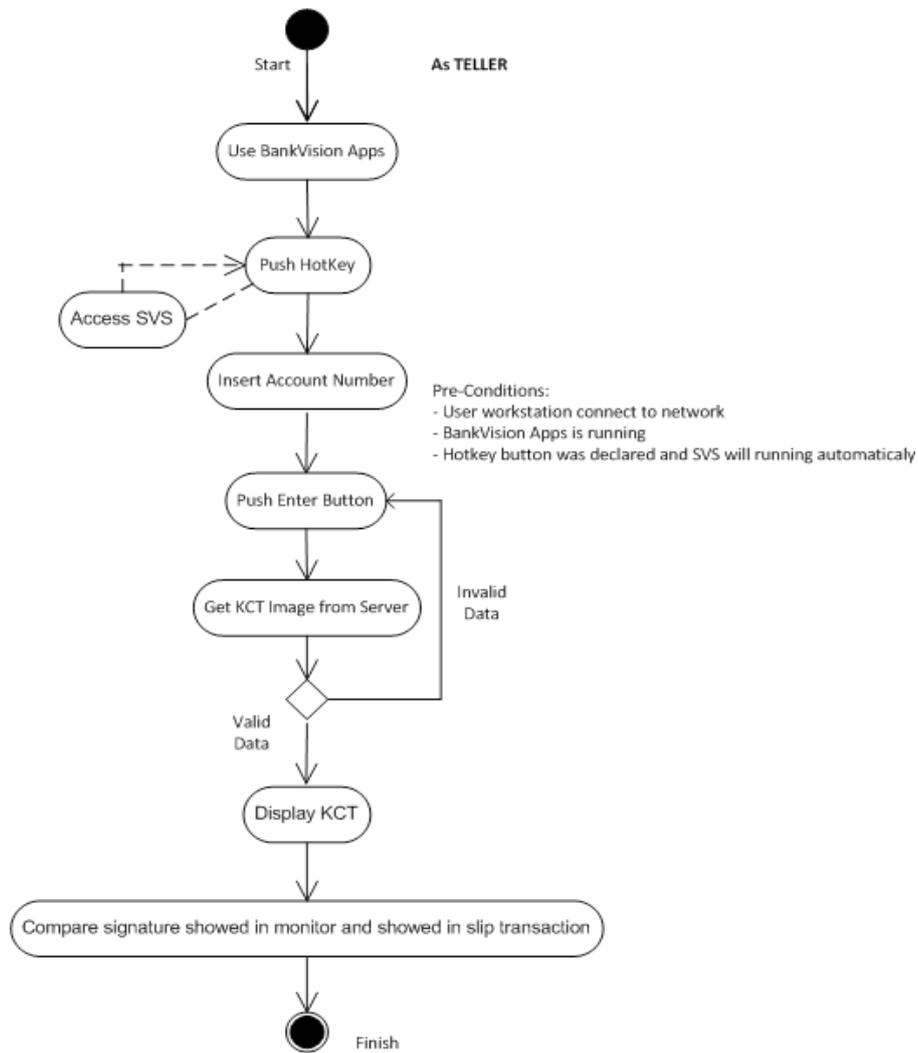
Gambar 5 Activity Diagram as Admin



Gambar 6 Activity Diagram as Maker



Gambar 7 Activity Diagram as Checker



Gambar 8 Activity Diagram as Teller.

## Communication Interfaces

Aplikasi SVS hanya dapat berjalan pada network yang saling terhubung antara *Server* dan *Client* (walaupun secara fisik berbeda lokasi). Proses waktu transfer data KCT (*retrieve*) dari *Server* ke *workstation* tergantung pada kecepatan *link bandwidth* dan ukuran *file* KCT itu sendiri. Kalkulasi Perhitungan Pengiriman data KCT sebagai berikut (Tabel 1):

Tabel 1 Kalkulasi Perhitungan Pengiriman Data KCT

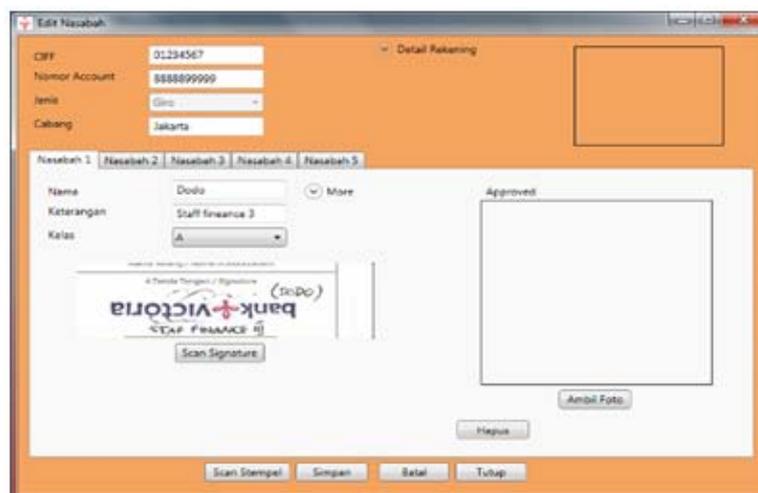
KCT Transfer Data Estimating Process		
Parameter	Nilai	Satuan
Ukuran KCT maksimal		1 MB
Bandwidth		64 kbps (dedicated bandwidth)
Durasi	= $(1000000 \times 8) / 64000$	second
	= 125	second

## Design Interface

Gambar 9 dan 10 di bawah ini merupakan rancangan antarmuka yang dibuat.



Gambar 93 Home Login.



Gambar 10 Edit Nasabah.

## PENUTUP

Sistem verifikasi tanda tangan secara *online* dipandang perlu untuk dijadikan sebagai sistem otentikasi yang cepat dan akurat. kartu contoh tanda tangan (KCT) didapatkan bagi setiap nasabah yang membuka rekening/*account* di bank, di mana kemudian KCT tersebut di *scan*, disimpan di dalam *Database* dan akan dijadikan sebagai alat verifikasi tanda tangan. Pemanfaatan sistem ini bagi sebuah bank dianggap penting untuk memastikan bahwa transaksi perbankan yang dilakukan oleh nasabah yang sebenarnya.

## DAFTAR PUSTAKA

- Bennet, S., McRobb, S., dan Farmer, R., (2002). *Object Oriented System Analysis and Design* (2nd Edition). London: McGraw-Hill.
- Deviani, Aireen. (2004). Analisis Dan Perancangan Sistem Verifikasi Tanda Tangan Secara *Online* Dengan Menggunakan Model BackPropagatio. Skripsi tidak diterbitkan, Universitas Bina Nusantara, Jakarta.