MENGENAL ELEKTRONIK BANKING

Oleh : Gunawan Hendro Cahyono, S.Kom *)

Abstrak

Semakin maraknya penggunaan selular khususnya pada smartphone, dimana sekarang ini yang namanya smartphone sudah bisa diperoleh/dibeli dengan harga yang terjangkau oleh semua lapisan masyarakat. Dan ditunjang pula dengan segala fasilitas yang diberikan oleh penyedia jaringan/operator selular, dimana sekarang ini penggunaan smartphone untuk akses data meningkat tajam. Keadaan ini dimanfaatkan dengan baik oleh penyedia layanan software dan juga oleh perbankan, sehingga sekarang ini orang belanja barang-barang cukup dengan duduk manis di rumah bisa pilih-pilih barang dan klik beli dan bayar, juga dengan hanya menggunakan menu/tombol-tombol yang sudah disediakan oleh penyedia layanan toko online. Selain untuk pembayaran online sekarang ini pihak perbankan sangat memudahkan nasabah untuk melakukan transaksinya secara elektronik, tanpa perlu dating ke bank dan teller, terkecuali transaksi cash. Saya akan mencoba membahas sedikit tentang metoda pembayaran online/elektronik dengan rekening bank yang kita miliki.

Kata kunci : e-banking, mobile-banking

PENDAHULUAN

Apakah yang dimaksud Pembayaran *Mobile*? Perangkat *mobile* sekarang ini mungkin telah mengubah pola bisnis dan kehidupan sehari-hari di bidang komunikasi dan transaksi keuangan, ponsel yang digunakan secara luas dan konsumen menjadi semakin akrab dalam menggunakan ponsel untuk berbagai keperluan seperti untuk transaksi keuangan melalui web site perbankan. Sebuah kesempatan baru yang muncul untuk penyedia layanan dan pedagang akan kelebihan dari sebuah ponsel sebagai dompet mobile. Mengingat keberhasilan layanan konten mobile seperti nada dering, game dan aplikasi lainnya, hal ini menjadi jelas bahwa konsumen bersedia untuk memanfaatkan ponsel untuk tujuan pembayaran. Ponsel juga memberikan kesempatan yang belum pernah terjadi sebelumnya untuk ekspansi aktivitas keuangan di negara-negara berkembang di mana jumlah pengguna telepon dapat melebihi jumlah mereka yang memiliki rekening bank.

Definisi dan Karakteristik :

Ponsel untuk pembayaran didefinisikan sebagai : "*Pembayaran untuk produk atau jasa antara dua pihak yang menggunakan perangkat mobile, seperti ponsel, memainkan peran kunci dalam merealisasikan pembayaran."* Pembayaran Ponsel dari transaksi antara konsumen dan pedagang yang melibatkan pembelian langsung barang dan jasa yang dapat berjalan baik dari Point-Of-Sale (POS)".

Pembayaran *mobile* dapat dikategorikan berdasarkan pada teknologi yang digunakan sebagai salah satu dari dua jenis pedekatan pembayaran. Jenis ini mendorong sifat model layanan pembayaran, nilai proposisi untuk kedua konsumen dan pedagang, dan teknologi yang relevan dan pertimbangan infrastruktur yang dibutuhkan untuk mewujudkan jenis pembayaran *mobile*.

Tabel 1 memberikan gambaran tentang dua jenis pembayaran tersebut.

Tabel 1—Tipe Pembayaran *Mobile*

Tipe	Teknologi yang digunakan	Penggunaan di seluruh dunia
Pembayaran langsung Pendekatan Pembayaran umumnya mengacu pada pembayaran contactless di mana credential pembayaran disimpan dalam perangkat mobile dan dipertukarkan melalui wireless, berbasis teknologi NFC, dengan terminal pembayaran berdedikasi dan kompatibel. Dengan kata lain, perangkat mobile bertindak sebagai kartu pembayaran contactless, sehingga menjadi faktor bentuk pembayaran baru. Pembayaran contactless juga dapat digunakan untuk jarak jauh; misalnya, untuk melakukan pembelian secara online dengan menggesekkan pada perangkat mobile melalui pembaca NFC contactless dicolokkan ke komputer pribadi (PC). **Pembayaran online** Terpencil pembayaran mencakup pembayaran yang terjadi baik melalui web mobile browser atau aplikasi smartphone, di mana ponsel digunakan sebagai perangkat untuk otentikasi informasi pribadi yang disimpan jarak jauh. Solusi pembayaran jarak jauh juga dapat digunakan untuk transaksi seperti tatap muka dan transaksi mesin penjual.	Ponsel yang digunakan oleh konsumen di toko untuk membayar barang atau jasa melalui reader contactless atau melalui berbasis teks atau berbasis personal identification-nomor (berbasis PIN), metode menggunakan Near Field Communication (NFC) technology melibatkan komunikasi antara perangkat konsumen, operator skema pembayaran, dan pedagang ritel di toko tersebut. Semua perangkat mobile NFC-kompatibel dapat mengirim serta menerima data sehingga ponsel NFC juga dapat bertindak sebagai pembaca kartu. Ini adalah teknologi yang sangat selaras dengan penggunaan media komputasi terpercaya seperti subscriber identity module kartu (SIM) dan Modul Trusted Platform (TPM). Ponsel yang digunakan oleh konsumen dalam kombinasi dengan layanan pesan jaringan seperti Short Message Service (SMS) atau Unstructured Supplementary Service Data (USSD) untuk membayar layanan atau konten digital. Pesan itu sendiri bisa digunakan untuk melakukan atau mengizinkan pembayaran atau dalam beberapa situasi bertindak sebagai unit mata uang atau pertukaran. Untuk transaksi bernilai rendah seperti pembelian nada dering atau ketika solusi otentikasi konten ponsel berdasarkan nomor identifikasi pelanggan mobile (MSIDN) yang digunakan, penagihan adalah melalui tagihan telepon pengguna. Nilai transaksi yang lebih tinggi dapat diolah dengan menggunakan berbagai pendekatan teknis seperti: • pembayaran berbasis kartu kredit / debit dengan memasukkan informasi pengguna melalui / pembayaran berbasis akun,	Sistem berbasis NFC yang baik digunakan atau diperiksa di daerah-daerah seperti Eropa Barat, Amerika Serikat, Kanada dan Jepang. Mereka juga mendapatkan penerimaan di negara-negara berkembang, khususnya dalam bentuk transaksi kartu contactless. Instalasi jenis ini adalah: ExpressPay ™ dari American Express, Discover® Jaringan ZipSM, MasterCard PayPass ™, dan Visa® payWaveTM dan SpeedpassTM. Pada bulan Juli 2011 PayPal™ memperkenalkan model pembayaran baru menggunakan NFC. Ini adalah varian dari model eWallet® di mana PayPal bertindak sebagai perantara yang transparan untuk pembayaran orang-ke-orang (P2P) yang memungkinkan pengguna Android™ untuk membayar satu sama lain dengan menekan dua perangkat berkemampuan NFC bersama-sama. Sistem SMS dan USSD menemukan aplikasi secara luas di Afrika dan di Timur Tengah di mana ada konsentrasi perangkat mobile yang tinggi, masyarakat pendatang yang besar dan penetrasi layanan perbankan yang rendah. Layanan pesan ini sedang digunakan untuk aplikasi seperti pembayaran kepada pedagang, pengiriman uang melintasi batas-batas nasional, dan pembayaran gaji bagi pekerja migran. Sebuah aplikasi luas dari jenis pembayaran mobile adalah penggunaan tarif SMS premium untuk pembelian nada dering, permainan dan barang lainnya. Sampai saat ini, jenis pembayaran biasanya digunakan untuk jumlah kecil (micropayment).

	nominal disimpan aman melalui antarmuka Wireless Application Protocol (WAP). • eWallet melalui antarmuka WAP aman. Dalam hal ini, kartu pengguna dan informasi rekening bank yang disimpan dengan aman pada perangkat pengguna mobile. Otentikasi berbasis PIN yang digunakan dalam hubungannya dengan transportasi memiliki respon suara interaktif (IVR), WAP, SMS dan saluran USSD. • aktivasi Aman pelanggan oleh penyedia layanan dan dipercaya memungkinkan dari hubungan antara MSIDN dan nomor kartu sangat penting.	

Saat ini, para pemangku kepentingan tidak jelas memisah peran dalam ekosistem pembayaran mobile. Lembaga keuangan dan operator jaringan mobile bersaing untuk entitas yang akan memegang rekening nasabah dan menerima porsi terbesar dari biaya. Lingkungan yang tidak jelas ini telah menciptakan jenis kategorisasi lain berdasarkan entitas yang memegang rekening nasabah bank-sentris dan nonbank-sentris.

Dalam model bank-centris, rekening nasabah yang dipegang oleh bank. Isu yang melibatkan hal-hal seperti kewajiban, pencucian antimoney, pemantauan transaksi untuk deteksi penipuan dan kepatuhan jatuh di bawah undang-undang perbankan lokal, nasional dan internasional yang sesuai dan peraturan. Ketika pembayaran dimulai, bank konsumen harus meng-otorisasi transaksi. Jaringan pembayaran yang digunakan adalah orang-orang tradisional seperti Visa dan MasterCard dan perbedaan utama adalah pada titik akhir transaksi.

Dalam model nonbank-centris, rekening pelanggan diadakan di organisasi non finansial seperti MNO atau layanan pembayaran pihak ketiga seperti PayPal. Dalam kasus seperti itu, yang penting peraturan, keamanan dan bahkan bagi hasil pertanyaan akan muncul. Misalnya, entitas yang akan bertanggung jawab untuk pengaturan layanan yang ini otoritas telekomunikasi nasional masing-masing atau bank nasional masing-masing?

Terutama di Uni Eropa (UE), pelonggaran pembatasan operator pembayaran yang mengarah ke perubahan dalam desain pembayaran *mobile* di seluruh Eropa. Secara khusus, pemain baru (operator seluler, department store, dll) akan diizinkan untuk diakui sebagai Penyedia Layanan Pembayaran (PSP) tanpa status lembaga kredit tradisional (sebagaimana didefinisikan dalam direktif Eropa 2000/12 / CE) dan untuk beroperasi dalam kompetisi langsung dengan lembaga keuangan / kredit tradisional, asalkan mereka memenuhi persyaratan yang ditetapkan dalam direktif. Secara khusus, mereka dapat bertindak sebagai Penerbit Uang Elektronik (EMI) 5 atau PSP.6 Mereka akan dapat menawarkan layanan seperti deposito tunai, tarik tunai, debet langsung, transfer kredit, pembayaran yang dilakukan oleh kartu atau perangkat serupa, dan kredit (untuk jangka waktu 12 bulan maksimum). Banyak pesaing yang sudah memiliki lisensi

penerbit uang elektronik di Eropa, dari raksasa internet seperti PayPal dan Google™, untuk start-up seperti Crandy, Luup atau Tunz. Beberapa operator telekomunikasi sudah memiliki lisensi perbankan, misalnya, Mobilkom di Austria, memiliki anak perusahaan dengan status keuangan, atau telah membangun kemitraan dengan PSP atau bank. Sampai saat ini, tidak ada inisiatif yang disebutkan di atas tampaknya akan di adopsi di seluruh dunia.

Saat ini, model pembayaran berbasis NFC bank sentris tampaknya menjadi yang paling umum dan, karena alasan itu, akan menjadi fokus utama dari tulisan ini. Ada sistem pembayaran non-bank-sentris yang digunakan, namun tingkat adopsinya belum begitu besar. Itulah yang terjadi, tulisan ini menyoroti fitur dan risiko pembayaran nonbank-sentris untuk ilustrasi sambil memfokuskan terutama pada isu-isu seputar kedekatan dan sistem berbasis NFC Bank-sentris untuk diskusi yang lebih besar.

Lingkungan Pembayaran Mobile

Lingkungan mobile payment melibatkan jenis berikut stakeholder :

- Konsumen
- Penyedia jasa keuangan
- Layanan Pembayaran penyedia
- In-service provider (pedagang), termasuk penyedia konten
- penyedia layanan jaringan
- produsen perangkat
- Regulator
- Standardisasi dan badan-badan industri
- Manajer Pelayanan Terpercaya
- Pengembang Aplikasi

Pemangku kepentingan ini dapat mengambil berbagai bentuk lembaga keuangan, debit / jaringan kartu kredit, kliring / organisasi pemukiman, penyedia solusi perangkat lunak, prosesor pembayaran pihak ketiga, MNO / nirkabel operator, produsen handset / chip pelanggan dan pedagang. Berbagai pemangku kepentingan yang berbeda berjuang untuk mengambil bagian mereka dari pendapatan dalam ekosistem baru dengan lembaga keuangan, jaringan debit / kartu kredit dan MNOs bersaing untuk peran FSP dan NSP dan untuk biaya transaksi terkait. Pembayaran contactless mobile adalah salah satu di antara banyak aplikasi. Sebuah gambaran global pemangku kepentingan utama dalam ekosistem NFC, dan peran mereka bisa bermain dalam waktu dekat, disajikan dalam paragraf berikutnya.

Beberapa contoh proposisi nilai bagi para pemangku kepentingan ini bervariasi adalah:

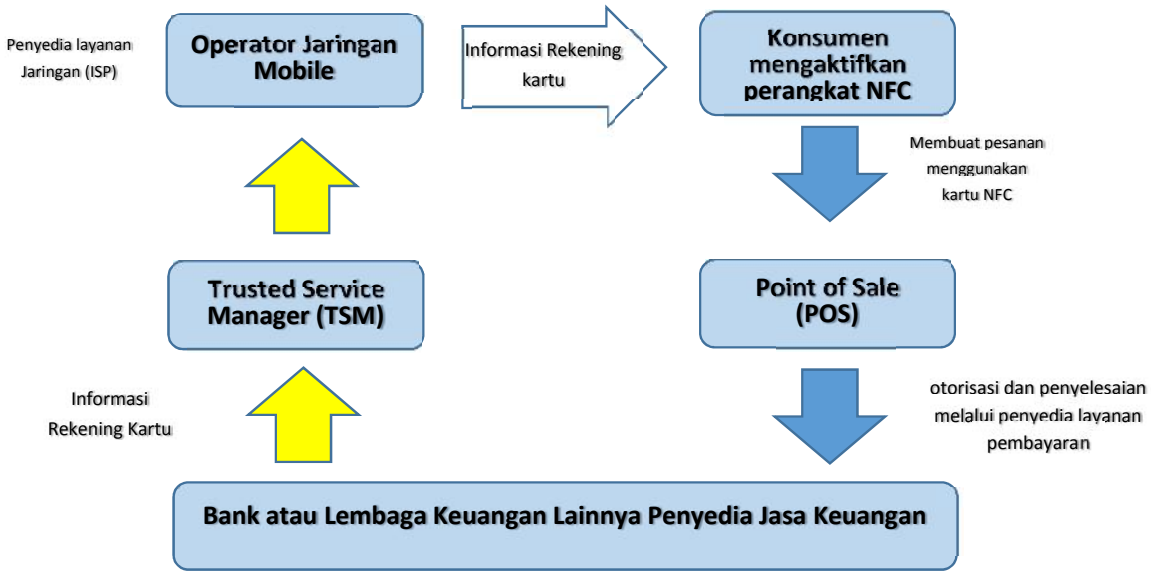
- Operator Ponsel Pembayaran Mobile contactless menyediakan sarana untuk menambah nilai penawaran komersial mereka dengan layanan baru, yang akan berpotensi, memungkinkan mereka untuk meningkatkan pendapatan rata-rata per pengguna (ARPU) akan menerima pendapatan baru yang bisa datang dari berbagai sumber, seperti biaya transaksi, menyewa ruang pada handset atau kartu SIM, lalu lintas data (terutama dari over-the-air [OTA] download), aplikasi penyedia layanan mengelola, dan menyediakan jasa keuangan .
- Bank-Mobile pembayaran contactless akan mengurangi cash handling (untuk micropayment) dan kartu plastik mengeluarkan biaya (untuk macropayment). Hal ini juga memberikan kesempatan untuk menawarkan layanan yang lebih interaktif, terkait dengan layanan perbankan online, seperti memberikan kredit pada titik pembelian.
- Pedagang Pembayaran Contactless membantu untuk mempercepat waktu transaksi serta menghasilkan transaksi lebih, terutama untuk pembayaran mikro,

dan juga mengurangi penanganan uang tunai. Pembayaran contactless ponsel juga bisa mengungkapkan peluang baru untuk program loyalitas, terutama dengan e-kupon yang dapat disimpan dalam handset dan dikonsumsi di kasir dengan menggesekkan telepon.

- Transportasi operator-operator. Banyak sistem transit sudah menawarkan kartu contactless untuk digunakan pada jaringan mereka. Karena infrastruktur sudah dikerahkan, sektor transportasi merupakan salah satu pilihan untuk meluncurkan layanan contactless bergerak dalam skala besar. Puting e-tiket ke ponsel membantu meningkatkan kepuasan pelanggan dengan membuat perjalanan harian lebih mudah. Dan mengganti tiket dan kartu contactless dengan aplikasi contactless yang dapat di-download ke handset secara signifikan akan mengurangi biaya tiket menerbitkan.
- Penyelenggara Tiket vendor-acara, museum dan bioskop yang menjual tiket melalui internet atau melalui jaringan seluler sekarang dapat mengirim tiket langsung ke pembeli melalui handset mereka NFC enabled, membuat pembelian tiket lebih cepat dan mungkin dari lokasi manapun. Selain itu, pembeli dapat cepat dilacak ke acara tersebut ketika mereka tiba, daripada menunggu di garis atau antrian. Penyelenggara acara juga dapat menggunakan aplikasi ini untuk layanan interaktif yang lebih, seperti memberikan informasi tambahan tentang acara tersebut.

Meskipun jelas bahwa potensi pembayaran contactless mobile signifikan bagi semua orang yang terlibat, ada pertanyaan mengenai model bisnis dan berbagi nilai.

Untuk memberikan beberapa konteks dan untuk lebih memperluas poin yang dibuat sebelumnya, tulisan ini mengambil melihat siklus hidup dari pembayaran mobile bank sentris NFC seperti digambarkan pada Gambar 1.



Gambar 1 Siklus Bank Penyedia Pembayaran Mobile NFC

Diagram diatas menggambarkan berbagai pemangku kepentingan yang terlibat dalam pembayaran mobile Bank-sentris. Ini menggambarkan juga arus informasi mengenai:

a) penyediaan informasi rekening pembayaran konsumen untuk telepon dari lembaga keuangan mengeluarkan (personalisasi perangkat) dan
b) otorisasi pembayaran mobile NFC melalui jaringan penyedia PSP yang ada. Arah panah menunjukkan transaksi pembayaran terkait, sedangkan panah diuraikan menunjukkan tindakan yang berkaitan dengan personalisasi aplikasi. Hal ini juga diasumsikan dalam gambar ini dan dalam model transaksi NFC perangkat mobile pengguna yang host chip NFC adalah platform yang terpercaya, yaitu, dengan menggunakan modul platform terpercaya (TPM) seperti yang didefinisikan dan ditentukan oleh Trusted Computing Group (TCG).

Sebuah pemangku kepentingan baru yang diperkenalkan dalam model NFC adalah Trusted Service Manager (TSM). TSM adalah pihak ketiga yang dipercaya yang (berpotensi) dapat digunakan untuk mengelola penyebaran aplikasi mobile. Seperti digambarkan dalam gambar 1, siklus hidup mobile payment termasuk TSM akan melibatkan berikut:

- Sebuah lembaga keuangan menyiapkan data akun dan mengirimkan informasi rekening pembayaran ke TSM.
- The TSM memberikan informasi rekening pembayaran konsumen melalui udara (OTA) melalui jaringan selular ke elemen aman di ponsel.
- Setelah rekening pembayaran di ponsel, konsumen dapat menggunakan ponsel sebagai kartu pembayaran virtual merchant yang menerima pembayaran kredit contactless dan debit.
- Dalam hal ini, pembayaran diproses melalui jaringan keuangan saat ini dengan kredit dan debet ke rekening yang sesuai.
- Jaringan operator mobile hanya digunakan selama personalisasi perangkat. TSM juga menangani siklus hidup perangkat sehingga mengelola federasi Data rekening nasabah antara ponsel dan menonaktifkan chip NFC dalam kasus pencurian.

Di seluruh dunia, ada sejumlah penyebaran pembayaran mobile di seluruh spektrum kedekatan dan pembayaran jarak jauh dan untuk kedua model Bank-sentris dan transaksi nonbank-sentris. Tabel 2 memberikan gambaran tentang jenis layanan pembayaran mobile yang disediakan dan yang mewakili ekosistem pembayaran mobile yang berkembang.

Tabel 2- Layanan Pembayaran Mobile

Tipe Service Provider	Contoh Aplikasi Jasa
Hybrid-kolaboratif	• Safaricom dan Vodafone (Afrika) meluncurkan layanan pembayaran berbasis SMS menargetkan tanpa memiliki rekening bank, pelanggan seluler prabayar di Kenya M-PESA. • Google Checkout™ (AS) kemitraan Google dengan Sprint®, Citi®, MasterCard, dan FirstData®
Operator jaringan seluler (MNO)	• PayBox oleh Mobilkom Austria-sistem berbasis SMS yang juga memiliki sistem NFC untuk mobile ticketing untuk transportasi ponsel • NTT DoCoMo, Inc (Jepang) Osaifu-Keitai® layanan mobile wallet
Layanan pembayaran Independen	• ObopayTM, Inc (AS) -A P2P perusahaan pembayaran mobile yang memungkinkan pengguna ponsel untuk mengirim dan menerima uang melalui ponsel mereka melalui web browser ponsel atau SMS • PayPal MobileTM (AS)-Menyediakan berbasis web dan PIN SMS kemampuan mobile untuk pembayaran rekening PayPal Aplikasi • Barat Union®-Mobile menyediakan P2P transfer uang dari rekening bank pengirim ke kartu ATM Western Union penerima

	• e-Transfer oleh Interac, Inc (Kanada)-Menyediakan kemampuan untuk mengirim dan menerima uang secara langsung dari satu rekening bank ke bank lain menggunakan online atau "mobile banking" melalui lembaga keuangan yang berpartisipasi tanpa berbagi informasi pribadi atau keuangan setiap

Beberapa poin penting yang perlu diperhatikan adalah bahwa masing-masing pihak memandang tanggung jawab dan kewajibannya berbeda, ekosistem membutuhkan peta jalan untuk mengidentifikasi infrastruktur dan fungsi yang diperlukan untuk mendukung konteks transaksi dan, yang paling penting, kesuksesan akan membutuhkan kerjasama dan interoperabilitas antara industri yang belum bekerja sama atau digunakan lingkungan bersama. Poin terakhir ini menyoroti fakta bahwa akan ada risiko bisnis dan risiko teknis yang dihadapi sebagai pembayaran mobile yang diadopsi, terutama dalam situasi di mana industri dapat menjauh dari model bank-sentris.

Manfaat Pada Bisnis dan Tantangan

Munculnya pembayaran mobile membawa berbagai manfaat baik dari perspektif bisnis dan konsumen. Ini termasuk:

- Kecepatan dan kenyamanan bagi pelanggan. Mereka tidak perlu membawa uang tunai atau kartu kredit.
- Cakupan Biaya-efektif tersedia di daerah pedesaan dimana tidak ada lembaga keuangan yang ada. Bahkan, bukti terbaru dari Filipina telah menunjukkan bahwa transaksi cabang bank khas biaya bank US $ 2,50, sedangkan transaksi pembayaran mobile biaya hanya US $ 0,50 (menurut laporan Asian Banker 2007).
- Kemampuan untuk mengirim uang ke luar negeri melalui (P2P) layanan pembayaran mobile orang-ke-orang. Dengan perkiraan 191 juta pekerja migran di seluruh dunia, dan dengan potensi bisnis pengiriman uang dari US $ 257 miliar di tahun 2005 (menurut PBB dan Bank Dunia, masing-masing), transfer dana internasional melalui ponsel merupakan peluang yang sangat besar untuk ponsel operator.
- The mobile wallet dapat mengkonsolidasikan banyak kartu. Ini menghilangkan kebutuhan untuk kartu fisik dan menyediakan satu jenis perangkat untuk semua aplikasi NFC (transportasi, membeli barang, dll).
- Peningkatan otentikasi melalui layanan berbasis PIN. Ini memberikan lapisan ditingkatkan keamanan.
- Ada kesempatan untuk mencapai sebagian besar penduduk bumi tanpa perlu investasi besar dalam teknologi. Penggunaan Ponsel yang lebih luas dari rekening bank, terutama di daerah pedesaan.
- Tidak perlu uang tunai bagi pedagang dan klien. Hal ini akan mengurangi resiko membawa dan mentransfer uang tunai, khususnya di lingkungan berisiko tinggi.
- Jumlah data yang disimpan diperlukan berkurang untuk memenuhi persyaratan kepatuhan.
- Kemampuan Smartphone seperti geolocation dan koneksi internet dapat digunakan untuk meningkatkan keamanan transaksi dan meningkatkan kemampuan mendeteksi kecurangan. Selain itu, kombinasi dari dua teknologi yang disebutkan sebelumnya dapat membuat jenis baru dari pemasaran, "geomarketing," di mana pedagang dapat menggunakan geolocation dan pembayaran mobile data untuk membangun profil pelanggan dan memberikan pengalaman pribadi.
- Realisasi yang lebih baik dalam kasus pencurian ponsel vs bahwa kartu kredit.

Konsumen cenderung lebih sadar ponsel mereka daripada kartu kredit mereka karena ponsel mereka adalah perangkat multifungsi dan oleh karena itu lebih sering digunakan.

- Mobile pembayaran membuka pasar bagi para profesional dan pedagang segmen rendah tanpa point-of-sale (POS) terminal. Ini adalah alternatif yang lebih murah daripada investasi di hardware untuk menerima pembayaran elektronik. Saat ini adalah aspek baru lahir pembayaran mobile yang dapat dari waktu ke waktu menjadi titik jual utama teknologi.
- Penggunaan counter smartphone menggelapkan metode yang menjelaskan sebagian besar penipuan kartu. Mereka juga memberikan perlindungan terhadap apa yang disebut pencopetan informasi dari kartu yang dilengkapi dengan identifikasi frekuensi radio (RFID).
- Remote Wipe fungsi banyak tersedia pada smartphone dan perangkat tablet, baik secara default atau sebagai sebuah aplikasi. Hal ini memberikan perlindungan pengguna informasi pribadi dan keuangan seharusnya perangkat mobile hilang atau dicuri.

Ada beberapa tantangan dan pertimbangan biaya/nilai bisnis ketika mempertimbangkan penggunaan layanan pembayaran mobile. Ini termasuk kesepakatan tentang model bisnis yang akan digunakan untuk pembagian pendapatan dan kepemilikan pelanggan, biaya retooling untuk mendukung pembayaran mobile seperti menggelar kemampuan NFC, dan ketidakpastian peraturan saat ini.

Kekhawatiran terhadap Risiko dan Keamanan

Secara historis, penipu telah menargetkan berbagai metode pembayaran dan ini mungkin menjadi kasus untuk pembayaran mobile; Oleh karena itu, analisis dimuka dan penanggulangan yang diperlukan untuk mengurangi risiko. Risiko dari perspektif pembayaran mobile dapat dikategorikan sebagai tradisional. Risiko tradisional melibatkan penolakan atau pencurian layanan dan kehilangan pendapatan, reputasi merek dan basis pelanggan sedangkan muncul risiko melibatkan penggunaan pembayaran mobile dalam pencucian uang dan pendanaan teroris.

Karena saat implementasi yang paling luas adalah model NFC Bank-sentris, risiko yang muncul saat ini adalah dari ruang lingkup tulisan ini dan oleh karena itu pembahasan saat ini akan fokus pada isu-isu risiko tradisional. Untuk diskusi tentang pencucian uang dan pendanaan teroris isu dan pendekatan mitigasi risiko, sumber yang sangat baik adalah dokumen "Integritas di Mobile Financial Services: Langkah-langkah untuk Mengurangi Risiko Dari Pencucian Uang dan Pendanaan Teroris" yang ditulis oleh World Bank.

Risiko bagi peserta dalam ekosistem pembayaran mobile tergantung pada peran entitas pengguna, jaringan atau operator komunikasi, atau penyedia layanan pembayaran. Beberapa entitas seperti MNOs mungkin memainkan dua peran tersebut secara bersamaan. Gambar 4 memberikan gambaran tentang jenis ancaman dan resiko yang mungkin ikut bermain di lingkungan pembayaran mobile di antara pemain utamanya.

Tabel 3- Risiko Pembayaran Mobile

Type Target	Kerentanan	Ancaman	Risiko	Penanggulangan
Pengguna	Melalui wireless (OT-A) transmisi antara telepon dan titik penjualan (POS) (NFC reader)	Intersepsi lalu lintas	Pencurian identitas, keterbukaan informasi, serangan replay	Modul dipercaya Platform (TPM), protokol yang aman, enkripsi
Pengguna	Instalasi sengaja perangkat lunak berbahaya di ponsel oleh pengguna	Download aplikasi mencegat data otentikasi	Pencurian parame-ter otentikasi, keter-bukaan informasi, penolakan transaksi	Otentikasi kedua pengguna (PIN) dan aplikasi (tanda tangan digital deng-an pihak ketiga yang terpercaya), TPM
Pengguna	Tidak adanya dua faktor otentikasi	pengguna menyamar transaksi	Penipuan, kewajiban penyedia	Otentikasi dua faktor
Pengguna	Mengubah atau mengganti ponsel	Konfigurasi dan setup kompleksitas	Mengurangi adopsi teknologi; "Keamanan dengan ketidakjelasan"	User interface yang disederhanakan, parameter keama-nan TPM ditetapkan oleh pihak yang ter-percaya
Pengguna	Smartphone In-ternet dan ke-mampuan geo-location	Malware pada pe-rangkat mobile; kontrol perlindung-an data miskin di merchant prosesor / pem-bayaran	Pengungkapan data dan pelang-garan privasi; profiling perilaku pengguna	user control fitur geolocation, privasi cryptographically didukung, modul platform terpercaya, dipe-riksa otorisasi dan akuntansi
Service Provider	Sistem POS me-nerima transmisi OTA	Pihak jahat banjir sistem POS dengan permintaan berarti	Denial of Service (DoS)	Permintaan filtering pada pembaca ber-dasarkan perangkat mobile-reader relatif geometri
Service Provider	Perangkat POS dipasang di tem-pat pedagang.	Menyamar serangan; merusak POS	Pencurian pela-yanan, replay, modifikasi pesan	POS Vendor pe-meriksaan, oten-tikator pesan, di-periksa otorisasi dan akuntansi
Service Provider	Kurangnya ma-najemen hak digi-tal (DRM) pada perangkat mobile	Ponsel pengguna perangkat ilegal mendistribusikan konten; misalnya, ringtone, video, game	Pencurian kon-ten, pembajakan digital, risiko penyedia un-tuk pelanggaran hak digital, hilang-nya pendapatan pe-nyedia konten atau pedagang	DRM yang terga-bung dalam desa-in TPM smartphone, kriptografi didukung DRM
Service Provider	Kelemahan dari Global System for Mobile Communi-cation (GSM) enkripsi untuk transmisi OTA; Data SMS dalam teks-jelas pada jaringan seluler	Modifikasi pesan, replay transaksi, penggelapan kontrol penipuan	Pencurian layanan atau konten, kehi-langan pendapatan, transfer ilegal dana	Protokol kripto-grafi yang kuat, otenti-kator pesan SMS, enkripsi

Strategi untuk Mengatasi Risiko

pembayaran mobile membawa peluang baru dan resiko baru. Transaksi pembayaran mobile dapat lebih terekspos risiko karena beberapa pihak yang terlibat dalam melakukan layanan pembayaran bersama-sama. Hal ini dapat memburuk jika layanan penting diserahkan kepada pihak ketiga yang berpotensi tidak diatur tanpa akuntabilitas yang jelas dan pengawasan, atau yang berada di luar negeri. Lingkungan transaksi multipartai ini kondusif untuk eksploitasi oleh penipu menggunakan serangan kedua teknologi dan sosiologis jika mekanisme perlindungan yang tepat dan kontrol akuntabilitas tidak didirikan di seluruh ekosistem mobile payment. Dengan perencanaan yang matang yang mencakup semua pemangku kepentingan, proses dan teknologi yang terlibat, ada kesempatan untuk membuat keamanan elemen intrinsik dari semua sistem pembayaran mobile.

Keuangan, pembayaran dan jaringan penyedia layanan (PJK, PSP, NSP) harus menerapkan pengamanan yang memadai dan program privasi dan tata kelola keamanan. Kurangnya pengaturan yang jelas tidak boleh digunakan oleh organisasi sebagai alasan untuk tidak bersikap proaktif. Terdapat risiko dari penyalahgunaan oleh pengguna yang berwenang seperti pencucian uang dan risiko penggunaan ilegal, daerah terakhir mungkin memerlukan dukungan dari undang-undang baru yang akan berkembang untuk memastikan perlindungan yang memadai. Setiap organisasi yang terlibat dalam rantai data transaksi harus menempatkan kontrol positif yang kuat untuk melindungi data tersebut saat berada dalam area nya.

Salah satu perhatian utama adalah memastikan bahwa transaksi yang dilakukan kemungkinan besar sedang dilakukan oleh orang yang berwenang atau terdaftar untuk melaksanakannya. Penggunaan otentikasi dua faktor akan memberikan kontribusi untuk perlindungan identitas yang lebih efektif bagi konsumen dan jaminan identitas yang lebih tinggi untuk pedagang. Dalam kasus transaksi NFC Bank-centris, perlindungan dari transaksi yang berasal dari pengguna yang tidak sah atau ponsel palsu dapat dicapai dengan menggunakan nilai verifikasi kartu dinamis (CVVs). Ponsel berkemampuan NFC chip yang mendukung ponsel CVVs dinamis dibandingkan dengan CVVs statis digunakan pada kartu strip magnetik. Jadi, jika ponsel palsu ini kemudian digunakan, akan menyajikan CVV salah dan transaksi tidak akan lolos, sehingga melindungi baik penyedia layanan konsumen dan atau pedagang. Demikian pula, jenis yang sama jaminan kepada konsumen harus ditetapkan di sisi merchant. Teknik analog untuk mengamankan socket layer (SSL) metode harus digunakan untuk memastikan bahwa POS atau jasa hanya sah jika penyedia dapat berinteraksi dengan ponsel. Titik-titik ini mewakili satu set yang lebih besar dari isu mengenai kepercayaan identitas dan kepercayaan untuk kedua pembayaran mobile dan mobile commerce pada umumnya. Masalah tersebut dan strategi yang potensial untuk mengatasi mereka yang dibahas, misalnya, pada tahun 2010 Gedung Putih publikasi pada strategi nasional Amerika Serikat untuk identitas terpercaya di cyberspace.

Faktor lain yang penting untuk dipertimbangkan adalah klasifikasi data selama transmisi dan penyimpanan data di berbagai node. Organisasi harus mengidentifikasi data yang dianggap pribadi dan sensitif dan harus memastikan bahwa mekanisme yang tepat berada di tempat. Juga, dalam hal data keuangan, segi yang sangat penting (selain dari enkripsi) adalah

masalah integritas data. Organisasi harus mempertimbangkan hal ini. Dalam hal data pembayaran mobile akan digunakan untuk layanan pemasaran, organisasi dapat ditemukan bertanggung jawab atas praktik bisnis yang tidak adil jika mereka menggunakan data pelanggan untuk tujuan yang tidak termasuk dalam persetujuan pelanggan.

Sama penting untuk dipertimbangkan adalah sistem POS dalam kasus pembayaran. Organisasi harus memastikan bahwa pihak ketiga yang berinteraksi memiliki sistim keamanan yang kuat. Selain itu, perhatian khusus juga harus diberikan kepada TSM, yang bertindak sebagai entitas yang "personal" chip TSM-kompatibel pada perangkat mobile vendor supplied. Dalam lingkungan cross-platform seperti kolaborasi, program pengendalian risiko organisasi harus memiliki fokus yang kuat pada pengelolaan layanan dari pihak ketiga.

ISACA Business Model untuk Keamanan Informasi (BMI) dan COBIT dan Risiko TI kerangka kerja memberikan pendekatan yang berguna bagi perusahaan untuk mengikuti menganalisis dan aktualisasi masyarakat, proses, teknologi dan perubahan organisasi yang terkait dengan penerapan pembayaran mobile. BMI dapat digunakan untuk membantu organisasi mengatasi konteks dan perlindungan data pembayaran mobile dalam organisasi. The COBIT dan Risiko kerangka kerja TI dapat diterapkan oleh suatu perusahaan untuk memastikan bahwa proses mitigasi pengendalian risiko yang efektif akan dibentuk mengenai penggunaan, pengumpulan dan tata kelola informasi pembayaran mobile tidak hanya dalam organisasi, tetapi juga untuk pengelolaan risiko yang timbul dari hubungan dengan pihak ketiga.

Akhirnya, seperti rantai hanya focus pada link terlemah, perhatian khusus harus diberikan pada titik yang berasal dari transaksi-perangkat pelanggan seluler dan pengguna. Pengguna harus dididik untuk memahami risiko yang sesuai. Perangkat selular manufaktur seharusnya tidak hanya bekerja sama dengan industri pembayaran untuk pengembangan platform yang memastikan lingkungan yang aman untuk melakukan transaksi mobile, tetapi juga interoperabilitas antara model smartphone yang berbeda sebagai pengguna cenderung sering mengubah atau memperbarui ponsel mereka. Penyediaan mulus layanan interoperable aman adalah sangat penting untuk keberhasilan pembayaran mobile.

Diskusi tambahan dari banyak titik-titik ini yang berkaitan dengan perangkat mobile dapat ditemukan dalam ketentuan ISACA (2010) tentang Mengamankan Mobile Devices.

Selain itu, dalam ekosistem baru ini, mekanisme kontrol yang dikembangkan oleh bank selama bertahun-tahun harus dimanfaatkan. Kontrol ini, ketika digunakan bersama dengan penanggulangan teknologi dan informasi yang dapat diperoleh dari transaksi seperti mobile geolocation dapat meningkatkan kepercayaan bahwa transaksi riil dan tidak penipuan. Apapun, transaksi juga harus tersegmentasi oleh jumlah pembelian, lokasi dan kategori merchant, dan risiko harus dikelola.

Tata Kelola dan Perubahan Isu

Penerapan sistem pembayaran mobile akan memerlukan perubahan dalam model bisnis dan proses serta infrastruktur teknologi yang mendasari yang terlibat. Pelatihan dan pengendalian internal yang baru harus dirancang dan dipantau. Seorang pengengali utama dalam penerapan layanan pembayaran mobile adalah model bisnis yang memberikan nilai kepada

semua pemain dalam ekosistem. Model bisnis dapat Bank-sentris, operator seluler-sentris, penyedia layanan-sentris independen atau hybrid-kolaboratif. Seperti disebutkan sebelumnya, publikasi ini difokuskan pada aspek bank sentris ekosistem mobile.

Dari perspektif model bisnis untuk kedua-bisnis-bisnis (B2B) dan (B2C) kegiatan bisnis ke konsumen, akan perlu untuk menjadi bekal untuk akses yang adil untuk segmen konsumen antara para pemangku kepentingan pembayaran mobile dan perlindungan konsumen yang memadai dan privasi. Manajemen hubungan suara pelanggan (CRM) akan memerlukan pengungkapan yang memadai dan tepat waktu risiko, tanggung jawab dan kewajiban yang terkait dengan transaksi mobile untuk pelanggan; dan identifikasi jalan bagi pelanggan dan pembentukan pengaduan penanganan prosedur internal dan cross-platform dan transaksi lintas-organisasi.

Akan ada kebutuhan untuk memodifikasi jaringan yang ada atau mengembangkan struktur jaringan baru untuk menyediakan interoperabilitas mulus yang akan dibutuhkan di antara para peserta dalam ekosistem pembayaran mobile, banyak yang belum memiliki interaksi langsung sebelumnya.

Karena sifat unik dari pembayaran mobile, penanggulangan organisasi individu tidak akan cukup, jadi perhatian khusus harus diberikan untuk interorganization hubungan dalam ekosistem pembayaran mobile. Sebagai contoh, sampai sekarang kartu pembayaran telah dikendalikan oleh sebuah organisasi atau lembaga keuangan. Sekarang, informasi kartu disimpan pada chip, misalnya, kartu SIM, yang dapat dipindahkan dari perangkat ke perangkat. Dan pelanggan mengubah ponsel, kehilangan ponsel dan membeli dari berbagai vendor yang tidak dikendalikan oleh bank. Situasi ini mengharuskan entitas baru diletakkan di tempat untuk mengatur chip yang tidak terkontrol dan untuk menjamin distribusi terpercaya informasi kartu pembayaran.

Sebuah solusi yang mungkin untuk memberikan mitigasi ancaman pembayaran mobile seperti pada tingkat sistem adalah untuk menyebarkan arsitektur TSM yang kolaboratif melintasi batas-batas teknis dan bisnis untuk memberikan inti dari ekosistem pembayaran mobile yang aman. Pendekatan seperti sedang aktif dievaluasi oleh beberapa bank nasional dalam diskusi dengan operator jaringan dan komunitas pedagang.

Dalam infrastruktur TSM berbasis TSM akan menjadi perantara netral untuk mengawasi bisnis dan operasional persyaratan untuk penyebaran skala besar dari pembayaran mobile. Fungsinya akan mencakup hal-hal seperti manajemen aturan bisnis dan otentikasi, menyediakan konektivitas antara MNOs dan penyedia layanan, memastikan end-to-end keamanan, menyediakan aplikasi manajemen siklus hidup untuk MNOs, handset dan pelanggan, dan dukungan pelanggan end-to-end. Beberapa keberatan dalam menggunakan pendekatan ini adalah bahwa TSM tidak akan berpartisipasi dalam proses transaksi NFC contactless yang sebenarnya, yaitu, transaksi akan diproses melalui saluran pembayaran yang ada dan TSM akan memfasilitasi otentikasi aman ke tepi jaringan sebelum untuk transmisi saluran yang ada.

Pertimbangan jaminan

Setelah memeriksa ekosistem mobile payment, peran para pemangku kepentingan dan sifat transaksi yang terlibat, dapat dilihat bahwa secara optimal untuk menentukan kriteria apa jaminan harus diterapkan (dan dalam konteks apa) adalah mempertimbangkan dua tingkat atau

derajat jaminan. Jenis pendekatan jaminan kepada layanan pembayaran mobile adalah fungsi dari peran yang terlibat. Secara khusus, hal ini dapat dicapai dengan:

- Menerapkan pengawasan kepatuhan perbankan tingkat penyedia layanan penanganan distribusi uang serta layanan pembayaran; misalnya, PayPal, Western Union, Google Checkout dan lotre sistem
- Menerapkan model standar audit dan standar untuk sistem pembayaran yang terkait dengan pembelian barang dan jasa; misalnya, MNOs, otoritas sistem transit dan pedagang eceran
- Jaminan profesional harus mempertimbangkan hal berikut ketika meninjau organisasi yang menyediakan layanan pembayaran mobile:
- kerangka COBIT ISACA yang dapat sangat berguna untuk layanan dan pihak ketiga penyedia karena memberikan dasar yang kuat untuk manajemen risiko, kepatuhan dan perlindungan yang tepat dan penggunaan mobile payment Informasi. Audit Mobile Computing Security ISACA yang / dokumen Program Jaminan menyediakan COBIT domain berguna dan proses referensi silang yang dapat disesuaikan secara langsung terhadap keamanan pembayaran mobile dan lingkungan audit dan konteks.
- Memastikan kepatuhan terhadap peraturan terkait yang mengatur kedua industri pembayaran dan industri telekomunikasi karena jenis baru ini pembayaran logis jatuh ke kedua kategori
- Hubungan kontraktual organisasi dengan TSM, kewajiban jaminan terutama bersama dan representasi
- The titik transfer kepercayaan dari Proses transaksi pembayaran mobile dan bagaimana dilindungi untuk memastikan kepercayaan end-to-end dari konsumen inisiasi transaksi untuk membeli pemenuhan, penyelesaian pembayaran.
- Perlindungan privasi dan integritas data transaksi dan rincian rekening pelatihan data pelanggan
- Kesadaran anggota organisasi untuk membawa risiko dan menangani tanggung jawab baru untuk model pembayaran mobile.

KESIMPULAN

Pasar pembayaran mobile adalah salah satu yang mengalami transformasi dan memegang masa depan yang menjanjikan bagi konsumen dan penyedia dalam dunia yang mengamati peningkatan layanan mobile berbasis teknologi smartphone. Beberapa poin kunci menarik bagi keamanan dan jaminan profesional, berdasarkan kondisi saat ini dan mengantisipasi masa depan untuk pembayaran mobile, yang dapat dicatat adalah:

- Kolaborasi dan model kompetitif untuk layanan pembayaran mobile yang diciptakan. Ada kemitraan baru-baru ini seperti Google dengan Sprint, Citi, MasterCard dan FirstData dan pengumuman Visa akuisisi Fundamo™, platform balik solusi pembayaran mobile di lebih dari 40 negara. Lintas-usaha tersebut dan cross-platform operasi akan diperlukan untuk pembayaran mobile untuk mendapatkan traksi dan akan membutuhkan adaptasi bisnis, keamanan dan jaminan model yang ada serta standar interoperabilitas direvisi atau peraturan yang baru.
- Keamanan dan privasi serta kenyamanan merupakan pendorong utama dari perspektif konsumen.
- Jaminan yang kuat dari pihak ketiga independen terpercaya serta pengembangan, dan kepatuhan terhadap, praktik bisnis terbaik dalam ekosistem pembayaran mobile akan diminta untuk mendorong adopsi pada konsumen secara luas. Kasus bisnis yang menarik

akan perlu dibuat bagi perusahaan untuk memperlengkapi kembali untuk mengakomodasi teknologi pembayaran mobile seperti NFC.

- Untuk saat ini masa depan yang menjanjikan dan menggiurkan, tapi pasti.

DAFTAR PUSTAKA

http://id.wikipedia.org/wiki/Near_Field_Communication

http://www.telecomspace.com/messaging-ussd.html

http://www.isaca.org/About-ISACA/Press-room/News-Releases/2011/Pages/New-ISACA-Guide-Offers-Tips-for-Secure-Mobile-Payments.aspx

http://en.wikipedia.org/wiki/Trusted_Platform_Module

www.sans.org/reading-room/.../**security-mobile-banking**-payments-3406

*) Ybs adalah Widyaiswara di Pusdiklat Migas