AIROME

CARA MUDAH MENGURANGI 75% PENIPUAN PADA BANK DIGITAL DALAM 3 BULAN

Ketika layanan finansial menjadi digital, nasabah bank digital tentunya menjadi titik paling rentan pada pengalaman perbankan. Sementara sistem bank itu sendiri terlindungi dengan baik, nasabah bank secara permanen diserang oleh penipu. Serangan besar yang dihadapi hampir semua bank adalah man-in-the-middle pada aplikasi mobile banking, phishing, social engineering, dan pembajakan OTP. Tujuan dari semua serangan ini adalah untuk mendapatkan akses ke rekening bank dan mengoperasikan keuangan.

APAKAH ANDA PERNAH BERPIKIR BAHWA MENGIMPLEMENTASIKAN SOLUSI AUTENTIKASI YANG BENAR, MAKA ANDA BISA MENGURANGI SEKITAR 75% PENIPUAN YANG TERJADI PADA BANK DIGITAL?

Berikut adalah deskripsi langkah demi langkah bagaimana kami mencapainya dengan PayConfrim yang diterapkan di 70 bank.

AUTENTIKASI SEPERTI APA YANG ANDA BUTUHKAN?

Untuk mengurangi sebagian besar risiko keamanan di saluran perbankan digital, ada beberapa hal yang harus diperhatikan. Solusi autentikasi harus melakukan enkripsi semua operasi — itulah sebabnya banyak solusi autentikasi berbasis OTP tidak sesuai dengan kriteria ini.

Harus ada yang melakukan non-repudiation dan kontrol integritas dari setiap operasi. Dari perspektif ini, apa yang disebut pendekatan WYSIWYS (apa yang Anda lihat adalah apa yang Anda tandatangani) sangat disarankan — jika tidak, bagaimana klien bank dapat memastikan apa yang sebenarnya dia konfirmasikan.

Jelas, solusi seperti itu harus mudah diterapkan dan dipelihara dan juga harus sangat mudah bagi nasabah bank. Pengalaman autentikasi omni-channel terpadu untuk klien juga merupakan salah satu poin penting bagi klien, juga bagi bank — lebih mudah bagi kedua belah pihak untuk menggunakan satu solusi yang sama untuk semua saluran, sedangkan untuk bank, cara ini juga hemat biaya.

PENGANTAR SOLUSI SINGKAT

PayConfirm adalah otentikasi perangkat lunak sepenuhnya solusi berdasarkan kriptografi asimetris. PayConfirm dapat digunakan untuk log-in, transfer uang atau apapun jenis konfirmasi aman pada saluran perbankan digital apa pun saluran: internet banking atau sistem manajemen kas berbasis web sederhana, mobile banking, operasi pembayaran kartu online, permintaan panggilan telepon atau bahkan ATM.

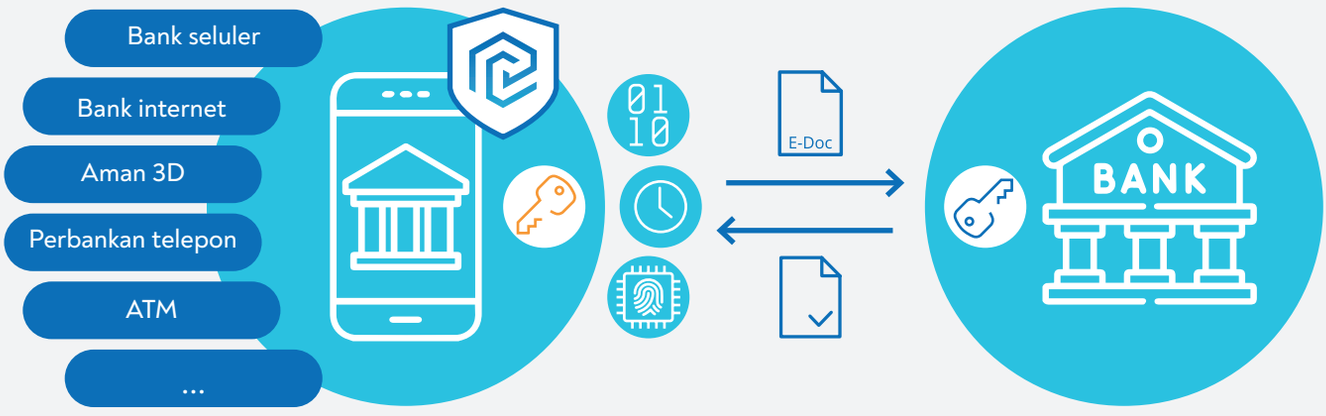
Secara teknis, ada pasangan kunci – kunci pribadi dan publik – yang dipisahkan antara server yang dipasang di sisi bank dan aplikasi mobile banking yang dipasang di perangkat klien. Kunci pribadi disimpan dengan cara terenkripsi ganda pada smartphone dan digunakan setiap kali klien mencoba mengonfirmasi transaksi. Kunci pribadi hanya dapat bekerja pada perangkat klien yang tepat, tidak dapat diekstrak. Kunci itu dilindungi dengan rahasia yang hanya diketahui oleh pengguna – bisa berupa kata sandi statis, Touch ID / Face ID.

Setiap konfirmasi dihasilkan hanya dengan satu ketukan pada layar smartphone sementara secara teknis itu adalah «tanda tangan» otentikasi yang dihitung secara kriptografis berdasarkan detail transaksi dan stempel waktu yang tepat, sidik jari perangkat yang tepat, dan nilai kunci pribadi. Semua informasi ini dikirim ke sisi server dengan cara terenkripsi yang diverifikasi dengan kunci publik.

Sidik jari membantu melakukan tautan dengan perangkat yang tepat – sehingga tim keamanan bank selalu dapat dengan mudah mengidentifikasi setiap upaya konfirmasi transfer uang dari perangkat yang berbeda.

Selain itu, dengan kesempatan ini hingga 70 parameter keamanan tentang perangkat akan tersedia untuk menghindari penipuan dan dipasang di dalam bank. Seperti melindungi dari setiap aktivitas yang berpotensi mencurigakan, malware yang diinstal pada perangkat, dll. Akan mudah diidentifikasi dengan fitur sidik jari perangkat. Dan juga akan mudah untuk mengidentifikasi upaya masuk ke akun pengguna dari perangkat yang berbeda.

Berdasarkan lebih dari 10 tahun pengalaman di internasional, PayConfirm menggabungkan pengalaman pengguna dan fitur keamanan yang kuat dan membantu melindungi dari sejumlah serangan paling populer seperti man-in-the middle, pembajakan OTP, social engineering, hingga phishing.



BAGAIMANA PAYCONFIRM DAPAT MEMBANTU DARI SERANGAN PHISING?

Phishing adalah jenis serangan ketika nasabah bank menerima SMS atau email yang bertujuan untuk meneruskan nasabah ke halaman palsu. Tujuannya biasanya untuk mendapatkan uang, mendapatkan detail data klien dan kemudian mengambil alih akun atau kadang-kadang — untuk memasang malware apa pun secara tersembunyi untuk membajak kode OTP bank atau melakukan tindakan apa pun untuk mendapatkan akses ke rekening bank nasabah

Sementara PayConfirm melakukan pemeriksaan kontrol integritas dan prinsip WYSIWYS (apa yang Anda lihat adalah apa yang Anda tandatangani), jika ada upaya untuk mentransfer uang, memberikan kredensial, mengubah nomor telepon pada akun, hal ini akan dengan mudah dideteksi pada langkah konfirmasi — nasabah bank hanya akan melihat operasi sebenarnya yang bersedia dia konfirmasi..

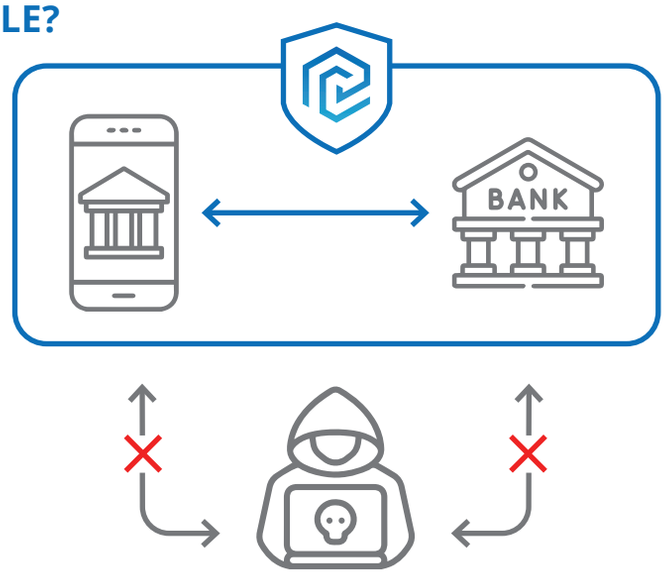
Pada saat yang sama, sidik jari perangkat akan membantu tim keamanan bank untuk mengidentifikasi malware apa pun yang terpasang di perangkat klien.

BAGAIMANA PAYCONFIRM DAPAT MEMBANTU DARI SERANGAN MAN-IN-THE-MIDDLE?

Man-in-the-middle (MIMT) telah ada beberapa tahun ini apalagi pada transaksi yang berhubungan dengan tablet dan laptop. Namun beralih ke layanan yang berpusat pada seluler, masalah penyadapan dan penggantian data dalam saluran komunikasi antara aplikasi perbankan dan sistem bank menjadi sangat penting bagi banyak bank.

Tidak masalah seberapa tepatnya penyerang dapat mengganggu saluran komunikasi — melalui kerentanan di sisi bank atau klien — dalam kebanyakan kasus, tanggung jawab akan berada di pihak bank.

Sementara solusi otentikasi sederhana berdasarkan OTP tidak dapat membantu dengan MIMT. Namun, dengan PayConfirm sangat berbeda. PayConfirm didasarkan pada asimetris kriptografi. Artinya ada pasangan kunci yang dipisahkan antara aplikasi dengan kunci privat dan server dengan kunci publik. Dengan demikian, semua data



ditransfer dari smartphone ke server dengan cara terenkripsi, sehingga hanya dapat didekripsi di sisi server menggunakan kunci publik.

BAGAIMANA PAYCONFIRM DAPAT MEMBANTU DARI SERANGAN SOCIAL ENGINEERING?

Dengan social engineering dalam hal ini yang kami maksud adalah semua panggilan yang diterima nasabah bank dari penipu yang memperkenalkan diri sebagai tim keamanan bank, tim humas nasabah bank, toko online apa pun dengan promo khusus. Tujuan penyerang ini adalah mendapatkan kode OTP untuk mentransfer uang, mengubah kata sandi akun, atau sekadar membeli sesuatu yang mahal atau bahkan voucher hadiah yang dapat dengan mudah ditukar dengan uang setelahnya.

Rahasia PayConfirm adalah tidak ada OTP atau kode lain yang dikirim ke klien. Bisakah Anda bayangkan scammer menelepon nasabah bank dan tidak mendapatkan apa-apa karena secara teknis tidak ada OTP yang dapat dibagikan dengan siapa pun?

Selain itu, jika ada upaya untuk mengubah kata sandi akun oleh scammer mana pun, hal ini juga akan diterima oleh nasabah sebagai permintaan otentikasi dengan keterangan detail: “seseorang sedang mencoba mengubah detail masuk akun Anda — apakah Anda akan mengonfirmasi bahwa itu benar-benar Anda?”

BAGAIMANA PAYCONFIRM DAPAT MEMBANTU DARI SERANGAN SIM-SWAP?

Sim Swap atau Pertukaran SIM adalah cara untuk menyerang nasabah bank yang bertujuan membuat tiruan kartu SIM untuk mengambil kendali atas akun pengguna. Tetapi jika bank menggunakan solusi otentikasi yang beroperasi secara independen dari lalu lintas operator seluler, saluran SMS, risiko serangan ini akan diminimalkan.

Ini adalah cara kerja dengan PayConfirm. Selain itu, dengan PayConfirm transaksi onboard dapat dikonfirmasi hanya dari perangkat yang tepat, karena sidik jari perangkat (karakteristik perangkat yang unik) adalah salah satu komponen penting yang digunakan selama konfirmasi transaksi.

BAGAIMANA PAYCONFIRM DAPAT MEMBANTU DARI PENIPUAN INTERNAL BANK?

Sedangkan di PayConfirm kunci pribadi digunakan sebagai salah satu komponen kunci konfirmasi transaksi dan disimpan di sisi klien, tidak ada pegawai bank yang dapat mengaksesnya atau menggunakannya untuk non-konfirmasi transaksi yang disetujui. Di sisi bank hanya ada kunci publik yang disimpan. Setiap kunci publik unik dan hanya dapat dicocokkan dengan kunci pribadi yang tepat dari pasangan kunci. Dengan pendekatan seperti itu menjadi mudah untuk membatasi tanggung jawab antara bank dan pengguna karena masing-masing pihak hanya bertanggung jawab atas kunci yang disimpan di pihak mereka.

Sedangkan setiap transaksi dapat dikonfirmasi hanya dari sisi pengguna dengan menggunakan rahasia yang diketahui atau disimpan oleh pengguna saja (kata sandi, touch ID/face ID)

BAGAIMANA PAYCONFIRM DAPAT MEMBANTU DARI PENIPUAN ATM?

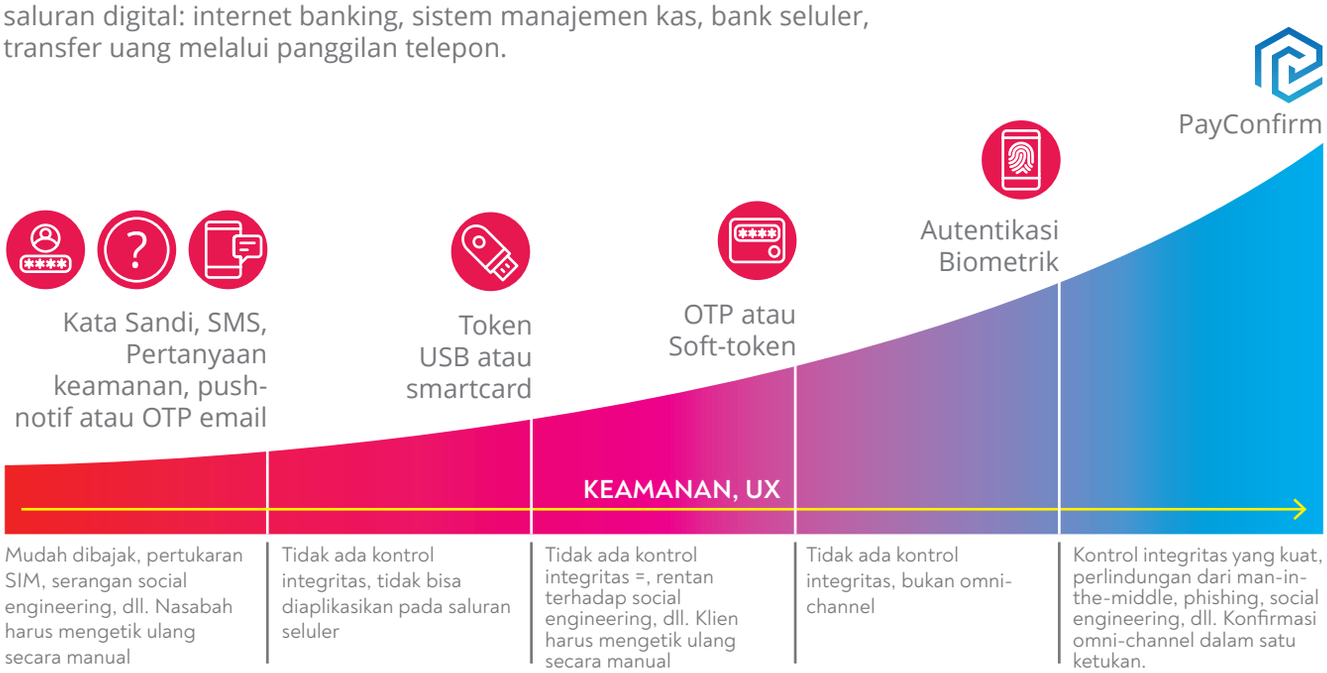
Salah satu cara penipuan ATM yang paling populer adalah skimming yang biasanya ada di sekitar kawasan wisata. Jenis serangan ini adalah upaya untuk mendapatkan detail kartu dan PIN atau menggesek data dari strip magnetik atau chip kartu. Inilah alasan mengapa banyak bank beralih ke opsi pembayaran seluler melalui kartu virtual dan mesin ATM berbasis NFC untuk menyediakan ATM tanpa kartu kepada klien mereka. Dalam hal ini pihak bank harus menyediakan biaya yang tinggi untuk peningkatan perangkat keras mesin ATM mereka, dan di sisi lain — tidak semua pengguna memiliki pembaca NFC di smartphone mereka.

Dengan salah satu fitur add-on PayConfirm — QR log-in — dimungkinkan untuk berinteraksi dengan ATM tanpa kartu fisik. Untuk log-in, nasabah menggunakan fitur pemindaian QR aplikasi perbankan, memindai QR dinamis di layar ATM dan mengonfirmasi operasi masuk dari smartphone dengan tingkat keamanan yang sama seperti pada kasus umum menggunakan PayConfirm. Interaksi lebih lanjut dengan ATM – penarikan uang – akan dikonfirmasi langsung melalui aplikasi perbankan di smartphone.

Dalam hal ini risiko penipuan kartu melalui saluran ATM diminimalkan tetapi pada saat yang sama tidak perlu meng-upgrade perangkat keras mesin ATM. Selain itu, nasabah bank mendapatkan pengalaman pengguna yang sama seperti dalam kasus lain.

KESIMPULAN

PayConfirm dapat memberikan solusi untuk kasus penipuan perbankan digital yang paling populer. Diimplementasikan di 70 bank secara global, belum pernah diretas. Poin bagus tentang PayConfirm adalah solusi otentikasi dapat digunakan universal untuk semua saluran digital: internet banking, sistem manajemen kas, bank seluler, transfer uang melalui panggilan telepon.



TENTANG KAMI

Airome Technologies adalah pengembang solusi keamanan siber yang berbasis di Singapura, dan kami berfokus pada perbankan digital dan sistem manajemen dokumen elektronik. Kami menyediakan perangkat lunak server-klien yang aman untuk mengonfirmasi atau menandatangani semua jenis operasi secara digital, termasuk transaksi bank atau dokumen elektronik, pada perangkat seluler. Tujuan kami adalah memberikan solusi untuk menurunkan risiko transaksi tidak sah yang disebabkan oleh serangan man-in-the-middle, phishing, atau social engineering.

Recognized by Gartner

BERHUBUNGAN BERSAMA KAMI

airome.tech
info@airome.tech