CVR-Token®

AUTHENTICATION SOLUTION

Powered by SHARING VISION™

www.sharingvision.com

Selama tahun 2015, serangan terhadap internet banking di Indonesia setidaknya sudah berevolusi dua kali.

Pada awal tahun 2015, serangan yang terjadi dikenal sebagai serangan **sinkronisasi token** yakni nasabah diminta memasukkan kode tertentu ke *token-device* dan kemudian memasukkan keluaran *token-device* ke halaman *web*.

Modus ini mengakibatkan kerugian hingga Rp 130 miliar menurut sumber POLRI yang kemudian dikoreksi oleh BI dan OJK menjadi kisaran Rp 5 miliar.

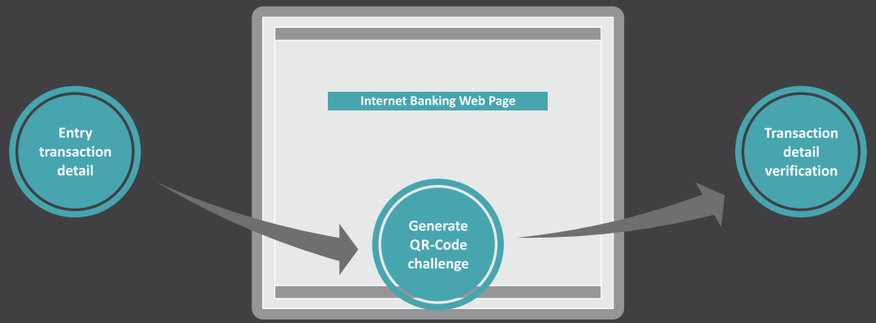
Serangan internet banking kembali berulang pada Agustus 2015. Serangan ini tidak lagi meminta nasabah untuk melakukan prosedur **tidak biasa**. Modus baru ini tentu lebih sulit dikenali oleh nasabah sehingga lebih rentan.

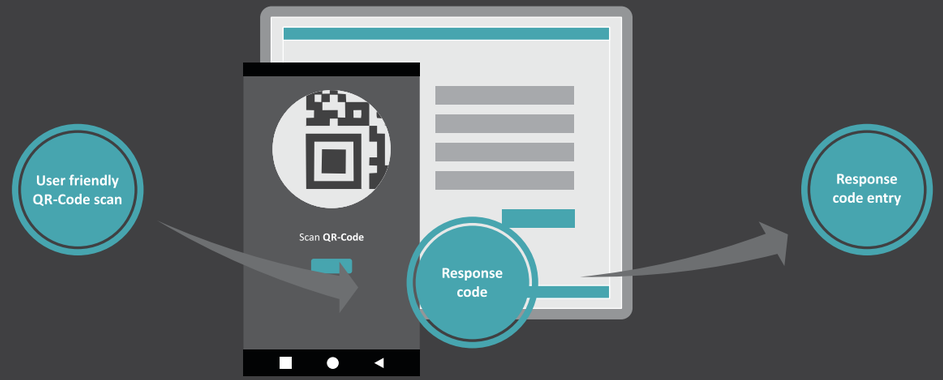
Seorang nasabah sebuah bank ternama mengalami kerugian hampir Rp. 50 juta setelah melakukan prosedur transaksi internet banking normal.

CVR-Token adalah **Soft-Token** pengaman transaksi *Internet Banking* yang didesain khusus untuk melindungi nasabah dari **man-in-the-middle-attack**

CVR-Token menggunakan mekanisme **challenge-verify-response** yang secara fundamental memperbaiki kelemahan token sebelumnya yang hanya menggunakan mekanisme *challenge* & *response*

LANGKAH TRANSAKSI DENGAN CVR-TOKEN





FITUR CVR-TOKEN

Secure CVR-Token Registration

Sistem memiliki mekanisme yang aman untuk melakukan instalasi dan registrasi **CVR-Token**.

Registrasi hanya dapat dilakukan oleh nasabah yang sah.

Strong Encryption Algorithm

Sistem dibangun dengan menggunakan berbagai algoritma enkripsi standar yang sangat kuat, diantaranya adalah: AES, RSA, SHA-256 dan memberikan layer *security* tambahan untuk menjamin keamanan proses otentikasi token.

Transaction Detail Verification

Nasabah dapat memastikan bahwa *challenge-code* benar-benar berkaitan dengan transaksi yang dimaksud. Modifikasi terhadap detil transaksi akan teridentifikasi oleh nasabah dengan cara memeriksa detil transaksi yang ditampilkan oleh **CVR-Token**.

Encrypted Challenge

Sistem memberikan *challenge QR-code* yang terenkripsi. Metode ini menjamin kerahasiaan *challenge-code*. *QR-code challenge* hanya dapat dibaca menggunakan **CVR-Token** sah yang telah terregistrasi.

Easy to Use

QR-code challenge sangat *user friendly* sehingga memudahkan nasabah ketika bertransaksi.

Preventing Client from MITM

Jika MITM terjadi, maka nasabah tetap aman dengan cara memeriksa kebenaran detil transaksi

Secure Verification Using Only Internet Connection

Nasabah tidak perlu menunggu detil transaksi yg dikirim lewat sms untuk memverifikasi transaksi.

Transaksi dapat diselesaikan hanya melalui *jalur data* yang digunakan untuk mengakses halaman *web internet banking*.

Comparison

	CVR-Token	Hard/Soft Token	SMS Token
Encryption	Encrypted challenge	Plain challenge	Plain response
Code Challenge	QR-Code	8 digit number	8 digit number for response
Transaction Detail Verification	Integrated	No	Could be sent via SMS
Client Prevention from MITM	Yes	Need out of band authentication (OOB)	Partially
Cost	No additional cost for device	There is additional cost for hard token device	There is cost for SMS charges

CVR-Token memberikan keamanan yang lebih baik untuk transaksi *internet banking* dan sekaligus memberikan *user-experience* yang sederhana dan mudah.

Contact Us

Intan Permatasari
intan@sharingvision.com
+628156021012

Budi Sulistyo
budi@sharingvision.com
+6281320574389

Powered by **SHARING VISION**™
www.sharingvision.com

Graha Sharing Vision Indonesia
Jl. Anggrek no. 47 Bandung 40114
T: +6222 7101403 F: +6222 7271057