eBanking:
Generating The Responses

by
k1m0ch1's

IDSECCONF 2010
INDONESIAN SECURITY CONFERENCE

Denpasar, 16 Oktober 2010

Who are us ?

- k1mOch1 (yahya.kimochi@gmail.com)
- Anton hilman (anton@hack.my)

Agenda

Ebanking : Generating The Responses

- Trend Keamanan Ebanking
- Security Token
- Mobile Token
- Challenge & Response code
- Generating The Responses
- Countermeasure
- Diskusi

Trend Keamanan Ebanking

- ❑ Sesuai Peraturan Bank Indonesia No. 9/15/PBI/2007 tentang penerapan manajemen resiko dalam penggunaan teknologi informasi oleh bank umum, maka diperlukan audit terhadap aplikasi perbankan untuk menjamin keamanan nasabah dalam melakukan kegiatan perbankan.
- ❑ "Security Token" sebagai pengaman tambahan bagi aplikasi perbankan, terutama bagi aplikasi transaksi finansial.

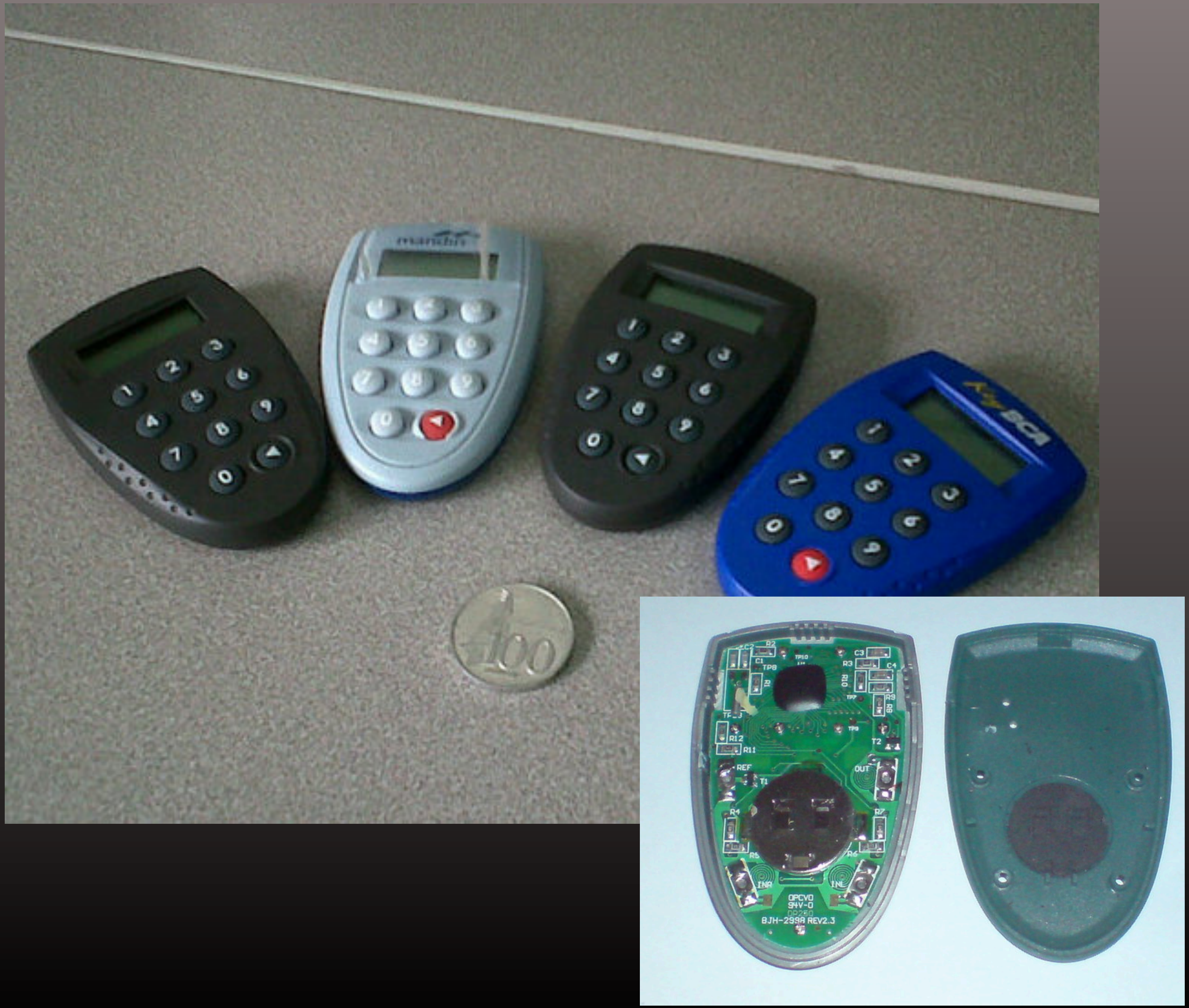
Security Token

Menurut wikipedia, bentuk dari Security Token diantaranya adalah :

- ❑ Static password.
- ❑ Synchronous dynamic password.
- ❑ Asynchronous password
- ❑ Challenge response

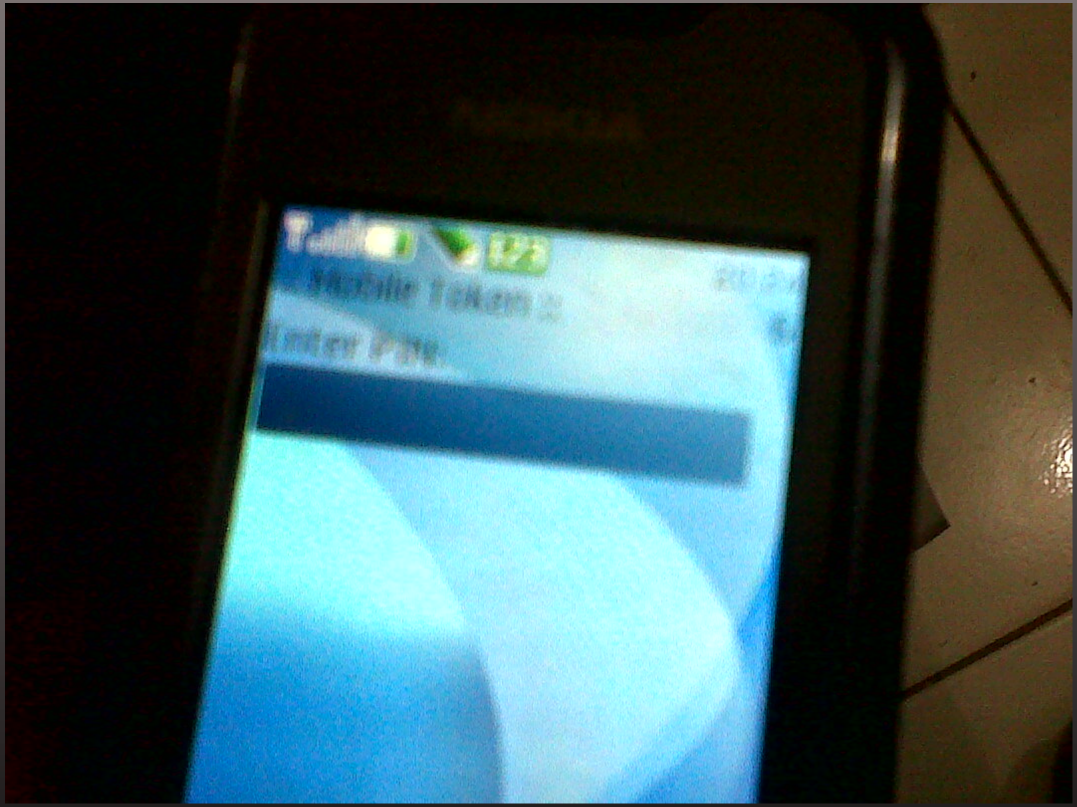
Security Token

- Hard Token

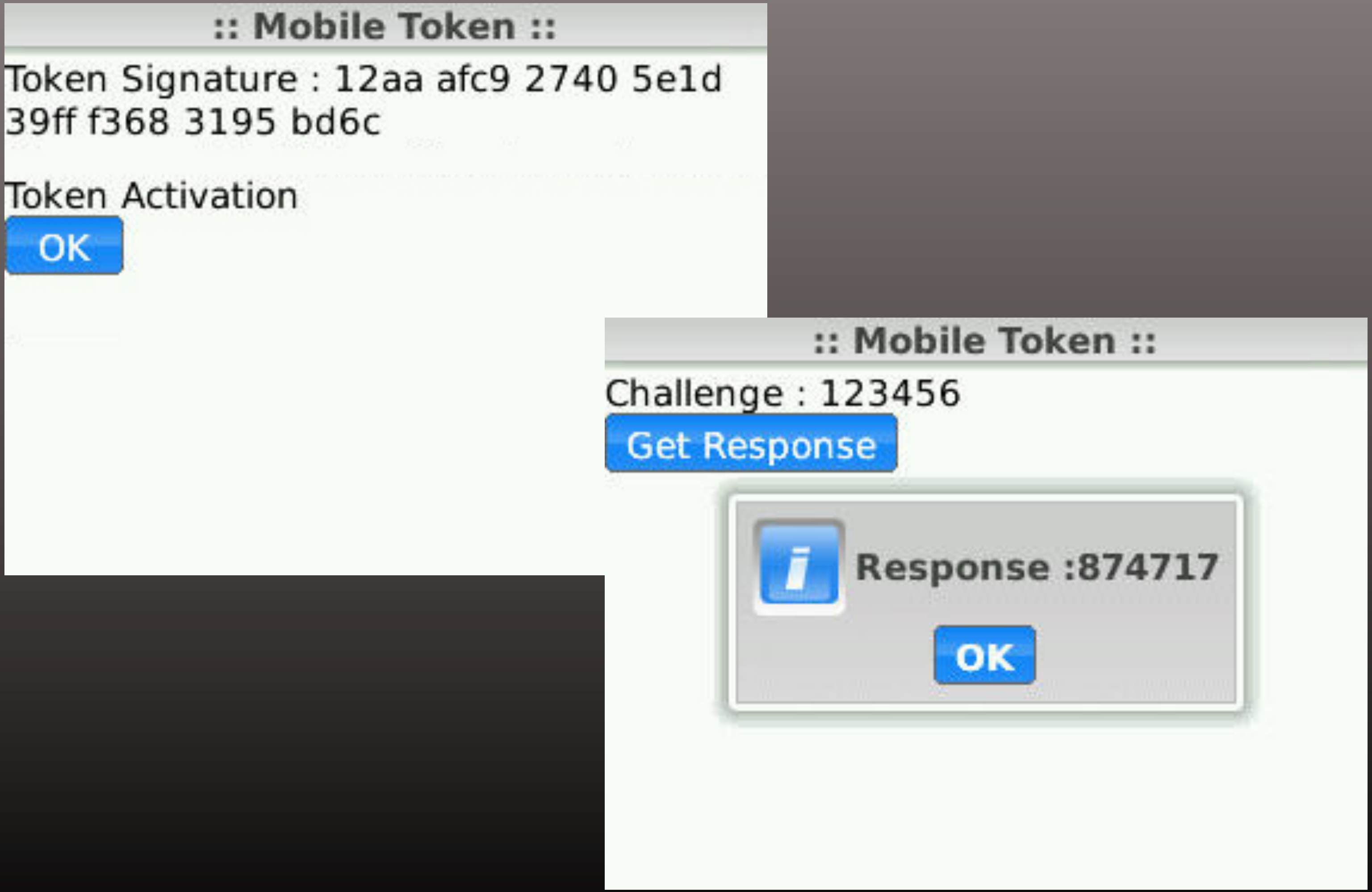


Security Token

- Mobile Token



Mobile Token



:: Mobile Token ::

Token Signature : 12aa afc9 2740 5e1d 39ff f368 3195 bd6c

Token Activation

:: Mobile Token ::

Challenge : 123456

Response :874717

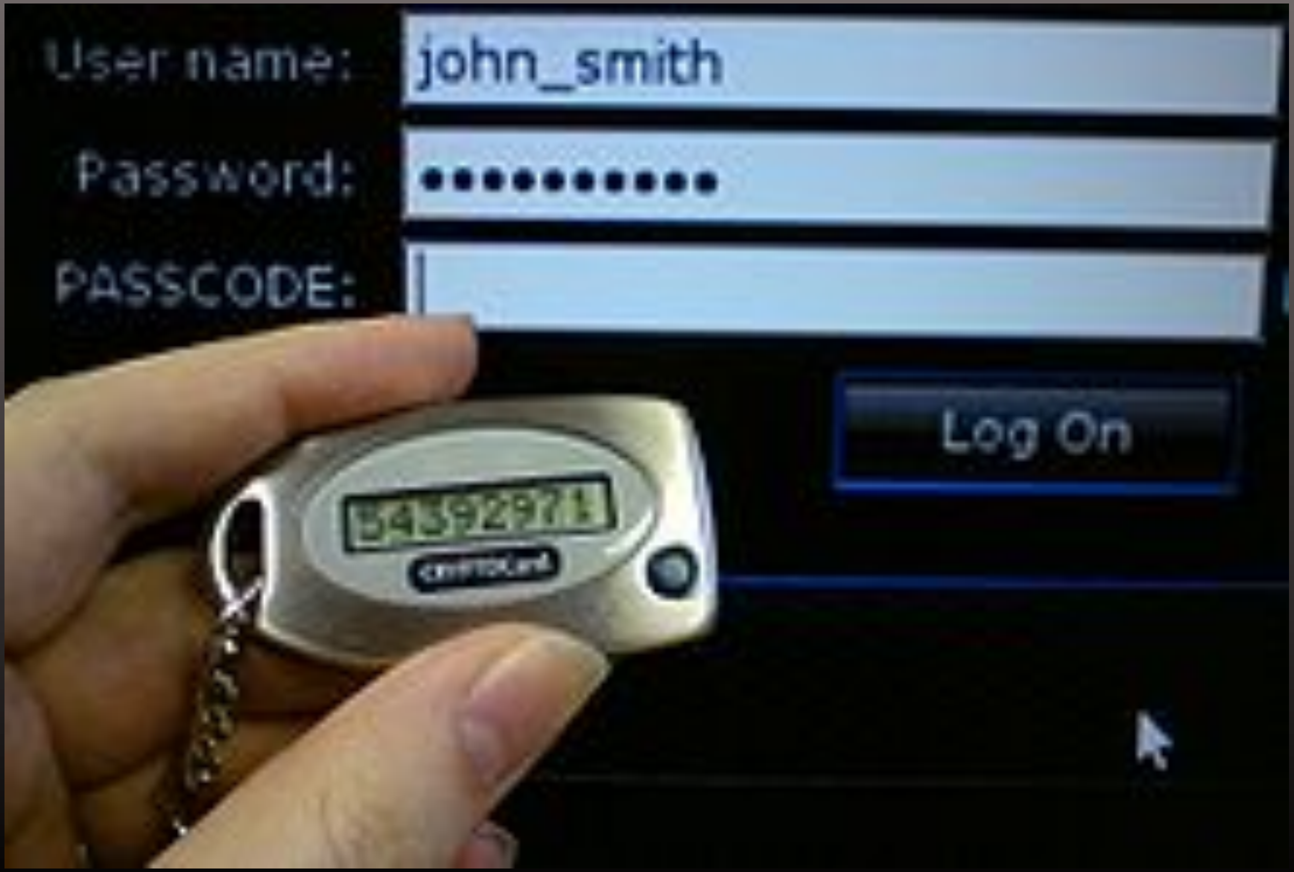
Challenge & Response Code

Prinsip dari Mobile Token

- Two Factor Authentification Security Device
- "Something You Know... Something You Have... Something You Are..."
- "Challengen and Response" (C/R) Mode for Authentification

Challenge & Response Code

“Two Factor Authentification Security Device”



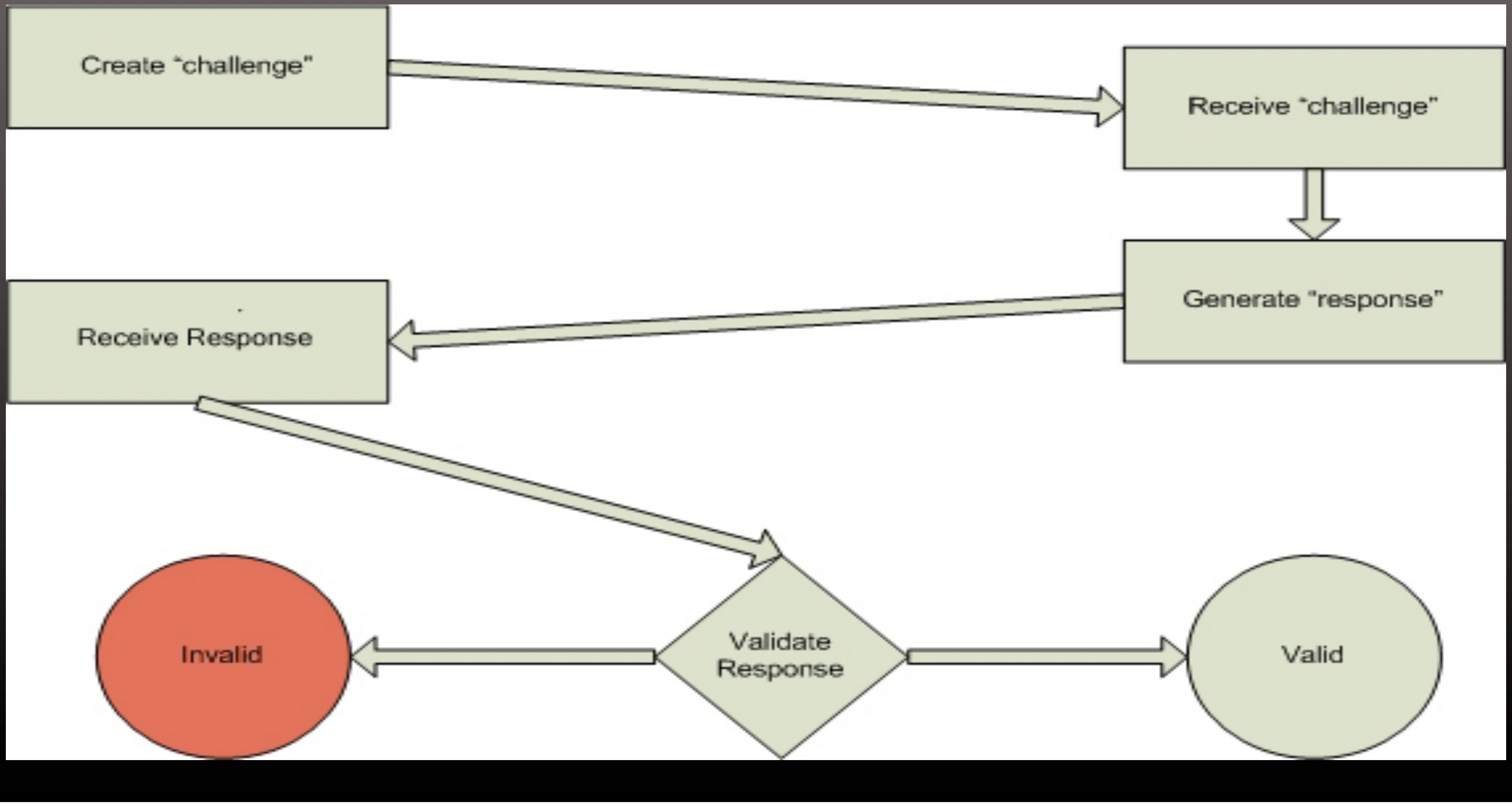
User name: john_smith

Password: ●●●●●●●●●●●

PASSCODE:

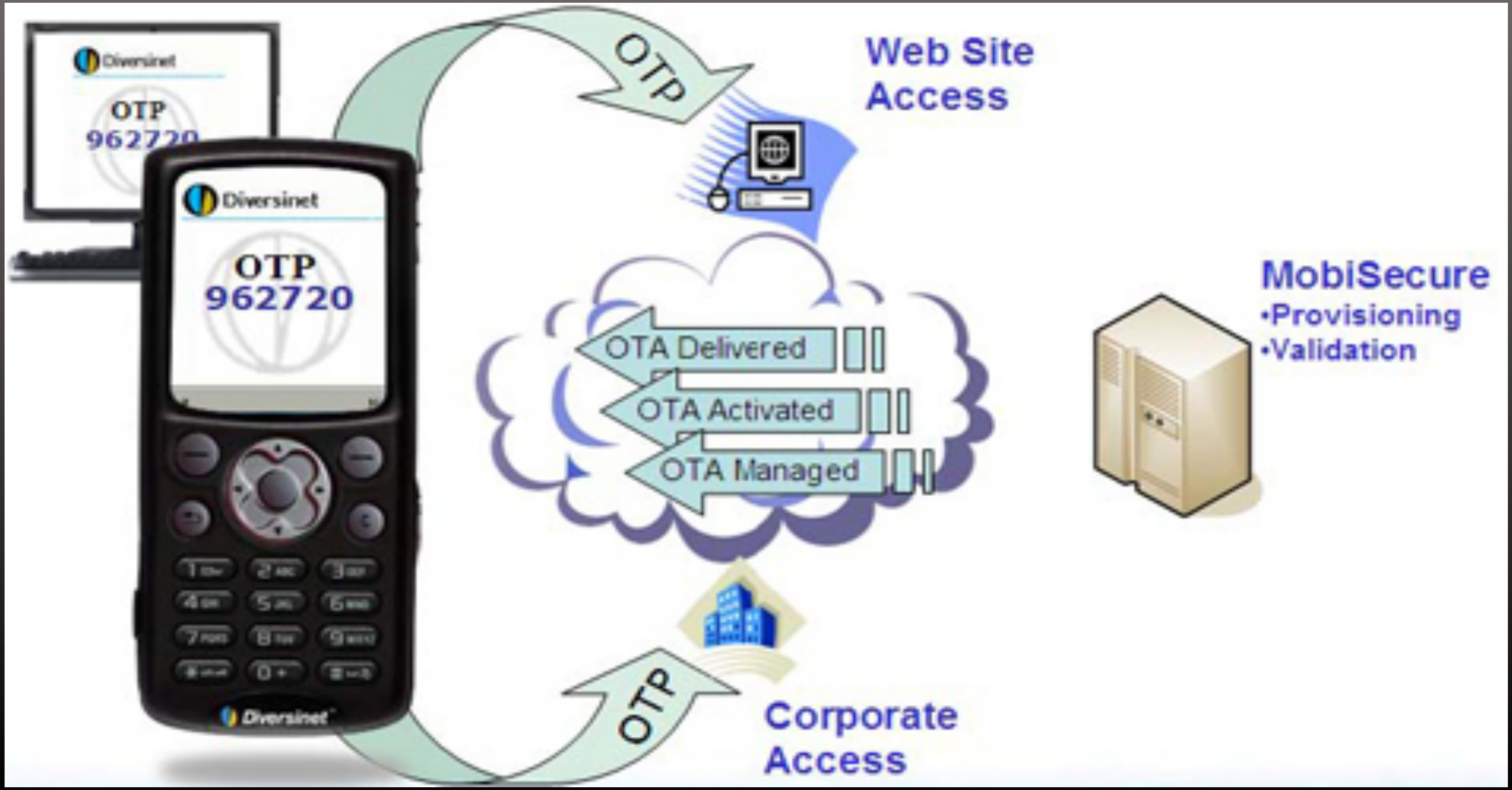
Challenge & Response Code

"Something You Know…
Something You Have…
Something You Are…"

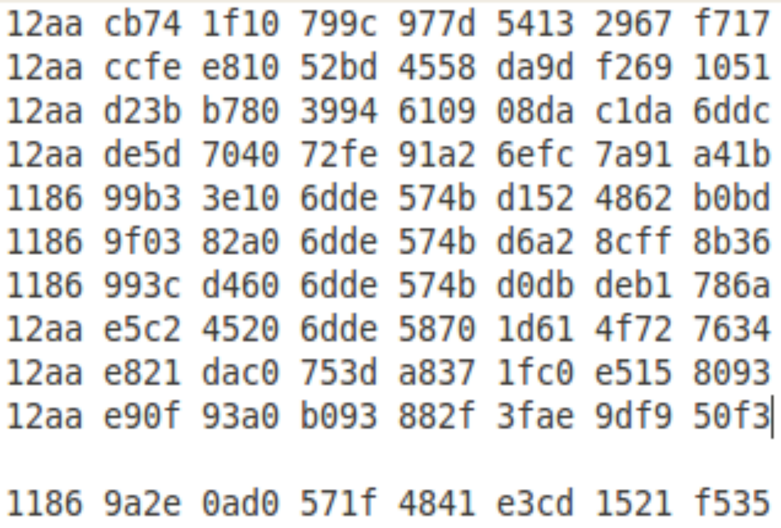


Challenge & Response Code

"Challengen and Response"
(C/R) Mode for Authentification



Generating the Response

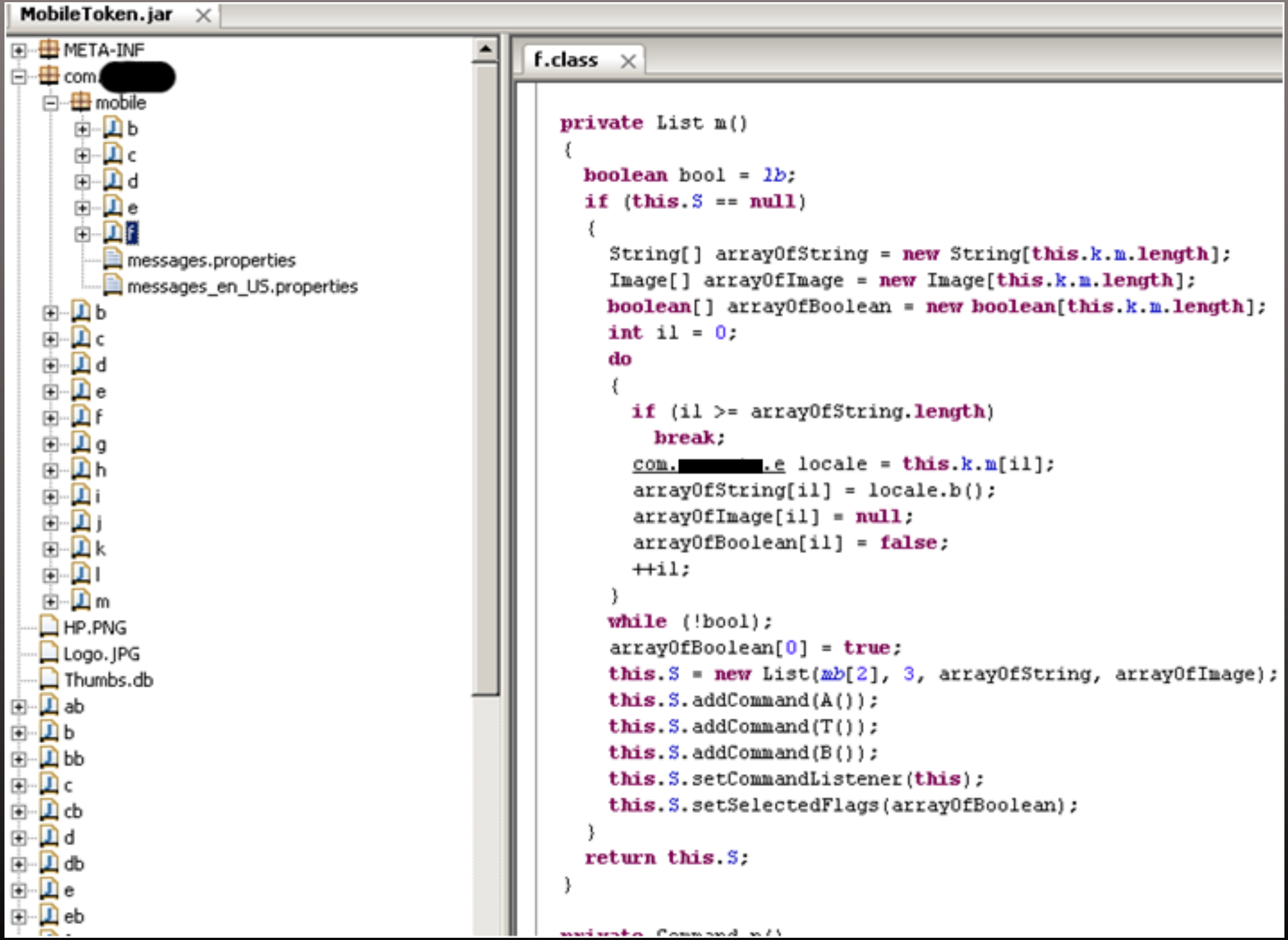


```
12aa cb74 1f10 799c 977d 5413 2967 f717
12aa ccfe e810 52bd 4558 da9d f269 1051
12aa d23b b780 3994 6109 08da c1da 6ddc
12aa de5d 7040 72fe 91a2 6efc 7a91 a41b
1186 99b3 3e10 6dde 574b d152 4862 b0bd
1186 9f03 82a0 6dde 574b d6a2 8cff 8b36
1186 993c d460 6dde 574b d0db deb1 786a
12aa e5c2 4520 6dde 5870 1d61 4f72 7634
12aa e821 dac0 753d a837 1fc0 e515 8093
12aa e90f 93a0 b093 882f 3fae 9df9 50f3

1186 9a2e 0ad0 571f 4841 e3cd 1521 f535
```

- Weak Algorithm
- Response tidak OTP
- Easly decompile

Decompile



```
private List m()
{
  boolean bool = 1b;
  if (this.S == null)
  {
    String[] arrayOfString = new String[this.k.m.length];
    Image[] arrayOfImage = new Image[this.k.m.length];
    boolean[] arrayOfBoolean = new boolean[this.k.m.length];
    int il = 0;
    do
    {
      if (il >= arrayOfString.length)
        break;
      com.[redacted].e locale = this.k.m[il];
      arrayOfString[il] = locale.b();
      arrayOfImage[il] = null;
      arrayOfBoolean[il] = false;
      ++il;
    }
    while (!bool);
    arrayOfBoolean[0] = true;
    this.S = new List(mb[2], 3, arrayOfString, arrayOfImage);
    this.S.addCommand(A());
    this.S.addCommand(T());
    this.S.addCommand(B());
    this.S.setCommandListener(this);
    this.S.setSelectedFlags(arrayOfBoolean);
  }
  return this.S;
}

private Command n()
```

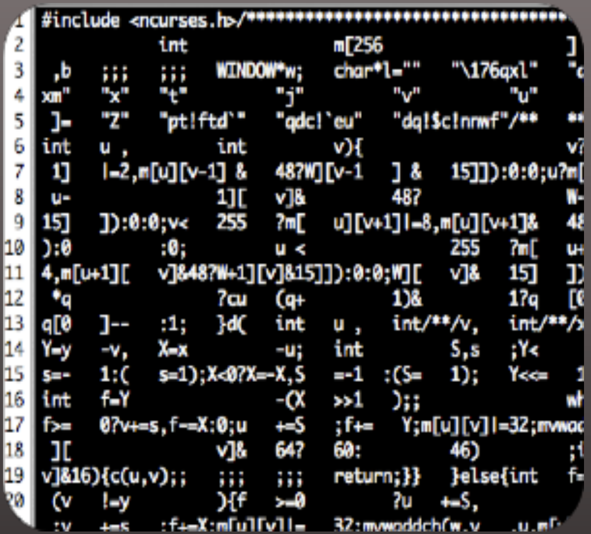
Countermeasures

Alternatif Solusi Pengamanan

- Application Hardening : Obfuscated Code, Encrypted Jar or Class, Executable Packer
- Parameter Setting pada Server

Countermeasures

Obfuscated Code

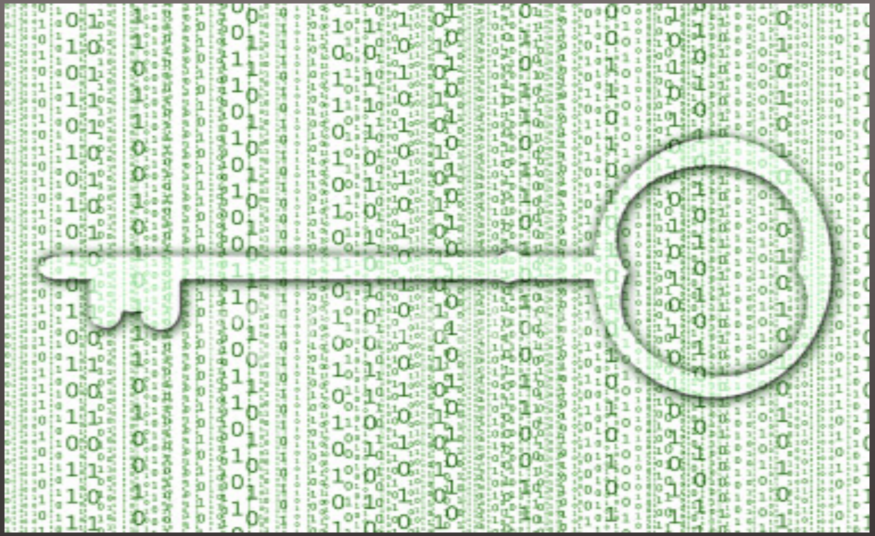


```
#include <ncurses.h>/*************************************
            int                 m[256                   ]
 ,b   ;;;   ;;;   WINDOW*w;   char*l=""   "\176qxl"   "c
xm"   "x"   "t"         "j"         "v"         "u"
 ]=   "Z"   "pt!ftd`"   "qdc!`eu"   "dq!$c!nnwf"/**   **
int   u ,         int         v){                     v?
 1]   |=2,m[u][v-1] &   48?W][v-1   ] &   15]]):0:0;u?m[
 u-               1][   v]&         48?               W-
15]   ]):0:0;v<   255   ?m[   u][v+1]|=8,m[u][v+1]&   48
):0         :0;         u <               255   ?m[   u+
4,m[u+1][   v]&48?W+1][v]&15]]):0:0;W][   v]&   15]   ])
 *q               ?cu   (q+         1)&         1?q   [0
q[0   ]--   :1;   }d(   int   u ,   int/**/v,   int/**/x
Y=y   -v,   X=x         -u;   int         S,s   ;Y<
s=-   1:(   s=1);X<0?X=-X,S   =-1   :(S=  1);   Y<<=  1
int   f=Y               -(X   >>1   );;                   wh
f>=   0?v+=s,f-=X:0;u   +=S   ;f+=   Y;m[u][v]|=32;mvwad
 ][               v]&   64?   60:         46)         ;t
v]&16){c(u,v);;   ;;;   ;;;   return;}}   }else{int   f=
 (v   !=y         ){f   >=0         ?u    +=S,
 ;v   +=s   ;f+=X;m[u][v]|=   32;mvwaddch(w,v   ,u,m[
```

- source or machine code that has been made difficult to understand
- Function Obfuscated
- Rewrite for as while, use special values

Countermeasures

Encrypted Jar or Class



- Use a tools to encrypt jar file
- Easier than obfuscated
-

Countermeasures

Parameter Setting pada Server

- Gunakan OTP (One Time Password) pada Challenge
- Penggunaan Salt
- OTP dalam mode self generated pada Response

Diskusi

Terima Kasih

yahya@ ccmandiri.com

sakitjiwa@antihackerlink.or.id