6 – 7 . APRIL ATLANTA, GA, USA

SYNERGY 2017

Building for the future. Better, faster, everywhere.

Time-base One-time Password

Eddy Kleinjan, Data Access Europe

Authentication

Authentication

- Strong Security measures becomes standard
- Make sure you know who you are dealing with
- Identify the party

UserID and Password

- Password should be kept a secret
- What if ...
  - Someone gets access to the password?
  - The users uses the same passwords in multiple places?

Use 2 Factor Authentication (2FA)

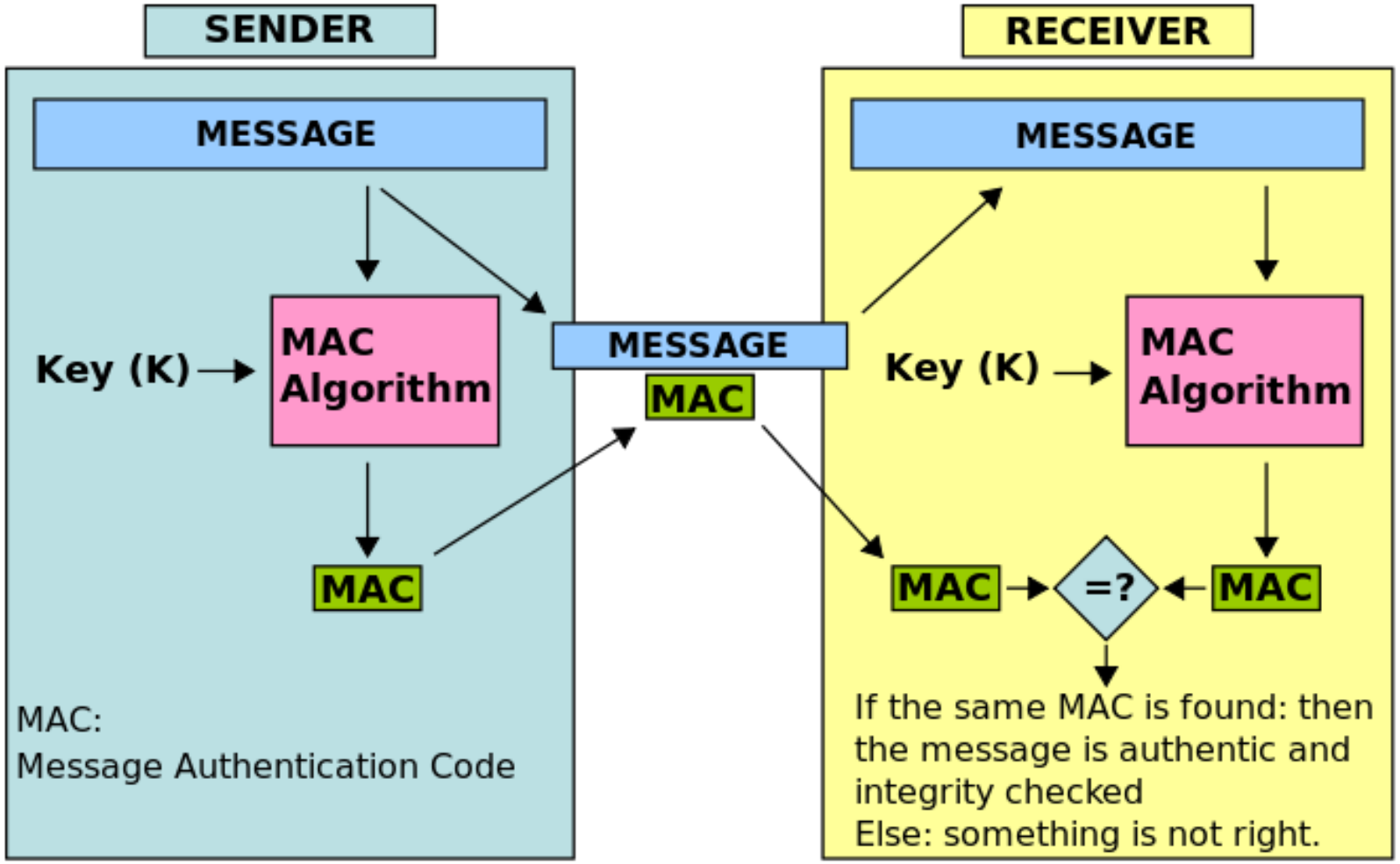
- 1: Something you **know**: User Id and Password
- 2: Something you **have**: Dynamically Generated Code on your phone

Where to use 2 Factor Authentication?

Time-based One-Time Password (TOTP)

- Internet Engineering Task Force standard RFC 6238
- TOTP hash-based message authentication code (HMAC)
- Basic Implementation
  - Takes a secret byte array as input; known by client and server
  - Takes the current time in a 30 second windows
  - Calculates a 6-digit code

Message Authentication Code



TOTP Generators

- SMS Text Message
- Token Generator Device
- Authenticator Mobile App

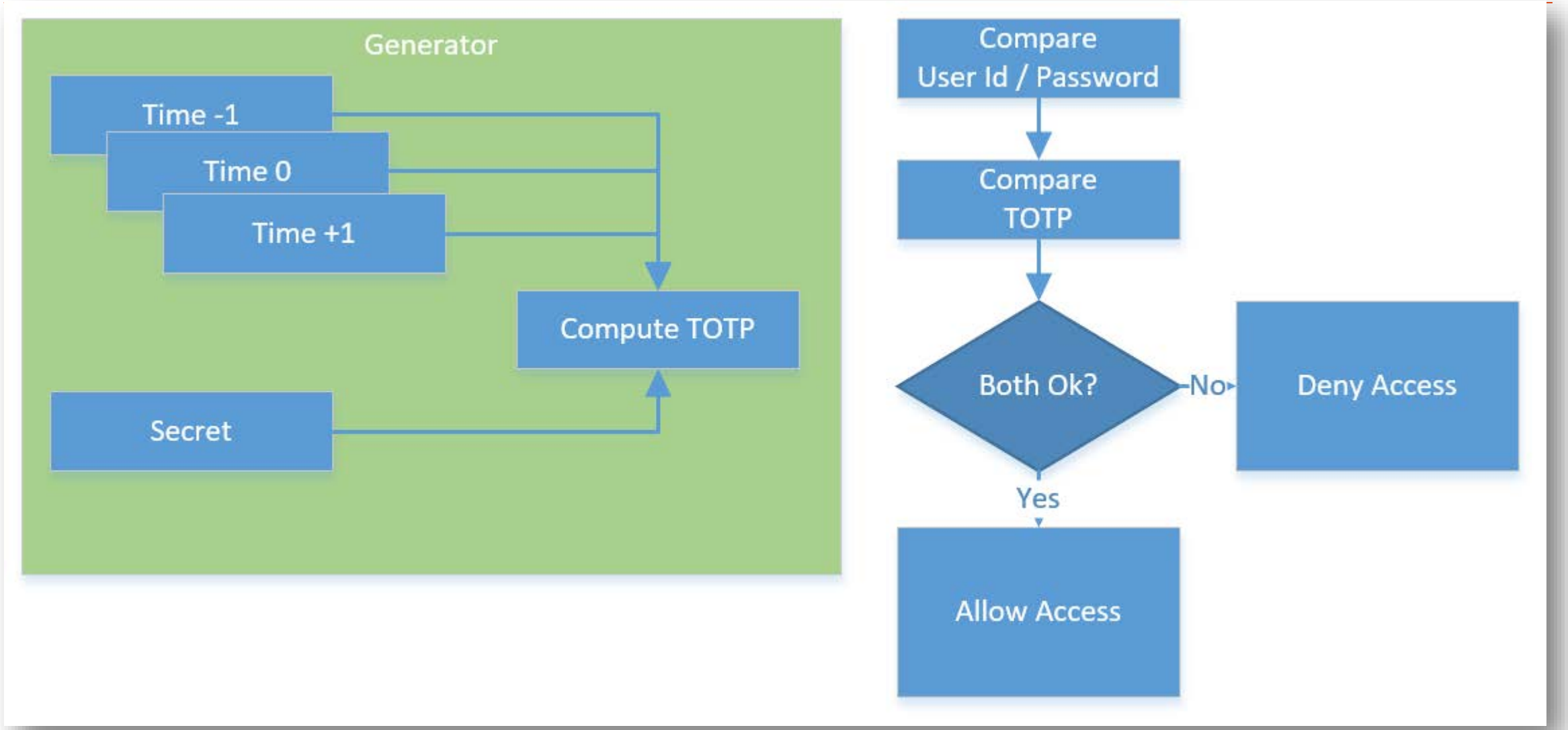
Client Side Authenticator Apps

- Google Authenticator 
- Microsoft Authenticator 
- Authy 

Client Side


Generator
Time
Compute TOTP
Secret
Authenticator
Promens Care
810 862
Eddyadm@pmcgw07.promens-care....
Microsoft
788 565
eddy.kleinjan@dataaccess.nl
DataFlex
102 352
login/guest
939 311
DataFlex
loginname
password
102352
sign in

Server Side


Generator
Time -1
Time 0
Time +1
Compute TOTP
Secret
Compare
User Id / Password
Compare
TOTP
Both Ok?
No
Deny Access
Yes
Allow Access

Let’s see…

cOneTimePassword.pkg

- Implements cOneTimePassword class
- Uses DLL for encryption and encoding logic

cOneTimePassword Properties

```
Property Integer piSecretCodeType otpDecodeNone
        Default None; options otpDecodeBase16, otpDecodeBase32 or otpDecodeBase64
Property Integer piDigitCount 6
        Default = 6 bit; options 6, 7 or 8
Property Integer piHmacType otpHmacSha1
        Default = otpHmacSha1; options otpHmacSha1, otpHmacSha256, otpHmacSha512
Property BigInt  piEpoch
        Default = 0; options 0 or 1
Property BigInt  piTime
        Default = 0 (now); otherwise number of seconds since unix time
Property BigInt  piStep 30
        Default = 30 sec; step size for factor
Property Integer piStepGraceCount 2
        Default = 2; Defines maximum number piSteps code may fall outside current
time when validating
```

cOneTimePassword Methods

```
// To get current TOTP value based on passed secret
Function TOTP    String sSecret Returns current TOTP Code

// To test entered Code; may be off by piStepGraceCount * piStep seconds
Function IsValidTimeBasedOneTimePassword ;
        String sSecret
        String sCode
        Returns True/False
```

Issue TOTP Details to User using URI

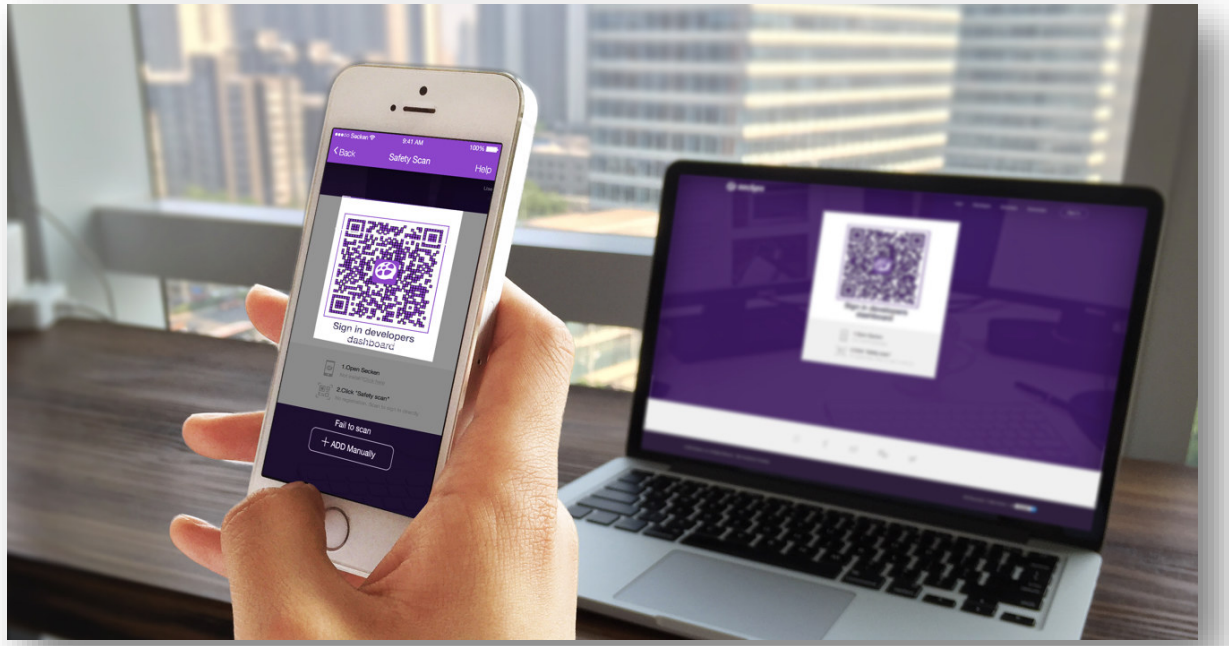
- Define the length of the code; **6**, 7 or 8 digits
- Define the encryption algorithm: SHA-1; **SHA-256**; SHA-512
- Define the time-window in seconds; default **30** seconds
- Share Secret Byte; **base32** encoded

URI:

otpauth://totp/DFAUTH:guest@dataflex?**secret=**7K7I7JYE3QTAUZXRB3ZRK32J5RLJU4MSUZOQMBSXEUXQRCO5C5SV====&**issuer=**DataFlex&**algorithm=**SHA256&**digits=**6&**period=**30

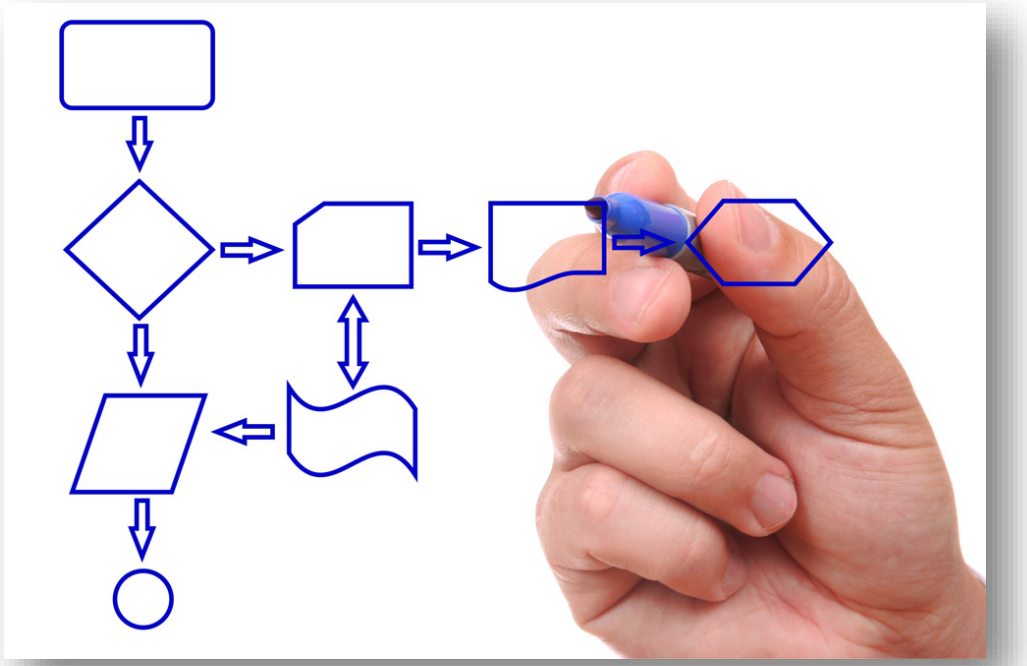
Issue TOTP Details to User using URI

- 7K7I7JYE3QTAUZXRB3ZRK32J5RLJU4MSUZOQMBSXEUXQRCO5C5SV====
- Generate QR Code for Ease of use
- Scan using Authenticator App



Implement procedures

- How to Issue Secrets?
- Re-Issue Secrets?
- Password Reset?



How to Issue Secrets

- Generate a Secret for each User

- Self Service on first-time usage or when switching devices
  - Send user an email containing a unique expiring link that shows the secret in text (for manual entry) and QR-Code
  - On the same page, let them enter the current TOTP based on the secret above to verify the installation
  - Register the new Secret with the user record

QR Code Control

```
Use cWebQrCode.pkg

…

Object oQrcode is a cWebQrCode
    Set piColumnSpan to 10
    Set piColumnIndex to 1
    Set psValue to ("http://whatever.url.or.info.com/bla")
End_Object
```

Questions?

Thank you!