

# One Time Password ບັນ ສຳຄັບປູໄວນ

MFEC Dev Day #2

MAHASAK PIJITTUM 2014-09-04



**เพิ่มความปลอดภัยในการทำรายการซื้อขายเงินออนไลน์ด้วย Verified by VISA  
Added Protection with Verified by Visa**

โปรดตรวจสอบความถูกต้องของข้อความนี้ยืนยันส่วนตัวของท่าน จากนั้นระบุรหัสผ่าน Verified by Visa  
เพื่อเพิ่มความปลอดภัยในการทำรายการซื้อขายเงินนี้

Please verify your Personal Message and submit your Verified by Visa password.  
You need to enter your Verified by Visa password in order to complete the transaction.

Merchant: [REDACTED]

Amount: [REDACTED] THB

Date: [REDACTED]

Card Number: [REDACTED]

Personal Message: [REDACTED]

กดท้ายคำว่า “Request OTP” เพื่อรับรหัสรักษาความปลอดภัย SMS-OTP  
Please click “Request OTP” to receive SMS-OTP password

OTP คือ อะไร!!!

กรุณาระบุรหัสรักษาความปลอดภัย SMS-OTP ที่ได้รับ  :  Request OTP  
Please input SMS-OTP password

[เปลี่ยนรหัสรักษาความปลอดภัยเป็นแบบธรรมด้า](#)  
[Change to static password](#)

# Static Password

VS

# Dynamic Password

“The system provides authentication for system access (login) and other applications requiring authentication that is secure against passive attacks based on replaying captured reusable passwords.”



“OTP is a password  
that is valid for  
only one login  
session or  
transaction.”

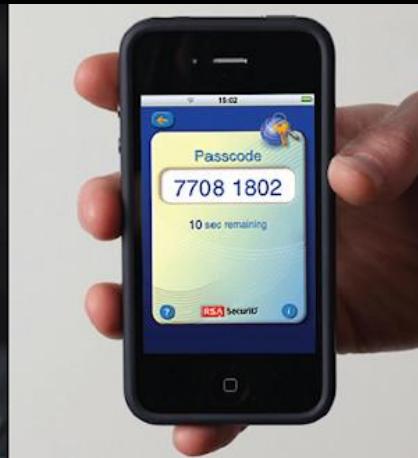


# Pseudorandomness

“a process that  
appears to be  
random but is not.”

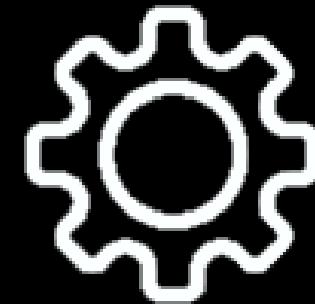


# OTP Delivery



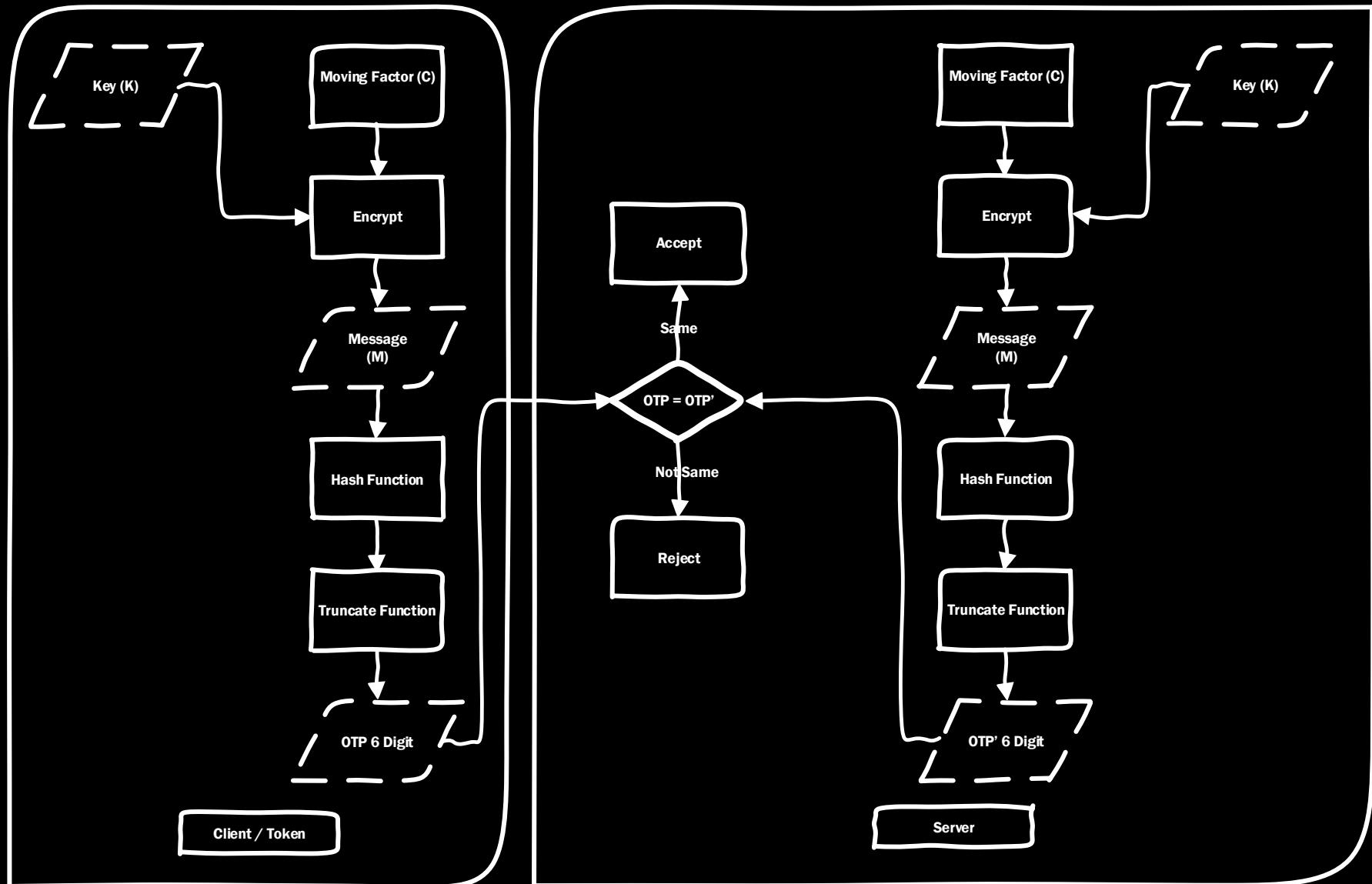
# OTP Generation Approach

- Time Based OTP
  - Time is moving factor
  - <https://www.ietf.org/rfc/rfc6238.txt>
- Event Based OTP
  - Event is moving factor
  - <http://www.ietf.org/rfc/rfc4226.txt>



OTP = Shared Key + Moving Factor

# OTP Generation Concept



Q & A