Dev(Talks): Bucharest, Romania

2015-06-11

An open source strong authentication server for less than $100!

André Liechti, CTO
SysCo systèmes de communication sa
(Neuchâtel, Switzerland)

http://www.multiOTP.net

oath
initiative for open authentication
CERTIFIED

Schedule

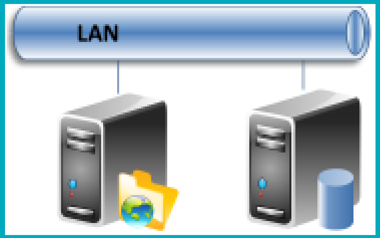
- Why regular passwords are never strong enough ?
- What about a different solution for more security ?
- **multi*OTP***, an open source library solution
- How to setup an authentication device for less than $100 ?
- Live-Demo with **multi*OTP*** installed on a Raspberry Pi
- Some questions ?

WHY REGULAR PASSWORDS ARE NEVER STRONG ENOUGH ?

(on the Internet, but elsewhere too…)

Why regular passwords are never strong enough ?

Same password for a lot of applications…



Some nice hardware tools…

Key logger…

Camera in car key…

… and some «nicer» hardware tools… ;-)

wireless Key logger…

fake USB Keyboard mounted in a memory stick…

and so on …

WHAT ABOUT A DIFFERENT SOLUTION FOR MORE SECURITY ?

What about a different solution for more security ?

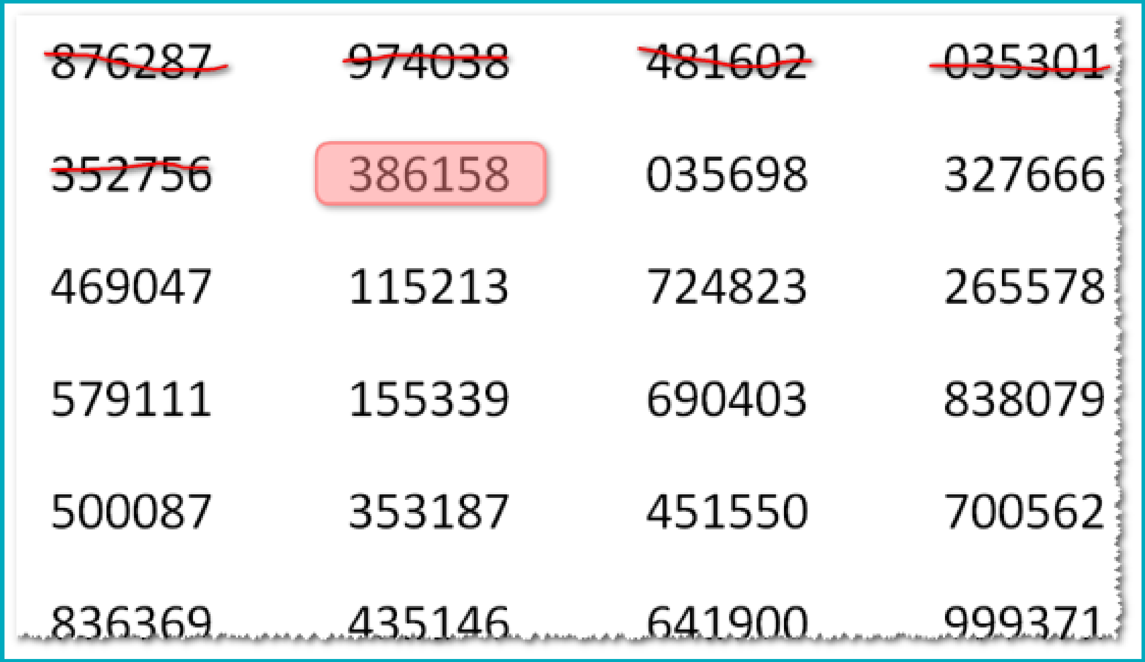
- Two-factor authentication
- A daily usage for the combination of knowledge and possession factors.

The ATM machine

– We have the physical ATM card **and** we know our personal PIN

Strong authentication with one-time password

- No software installation is required for the user (compatible with all OS and Internet navigator)
- Secret PIN + scratch passwords list



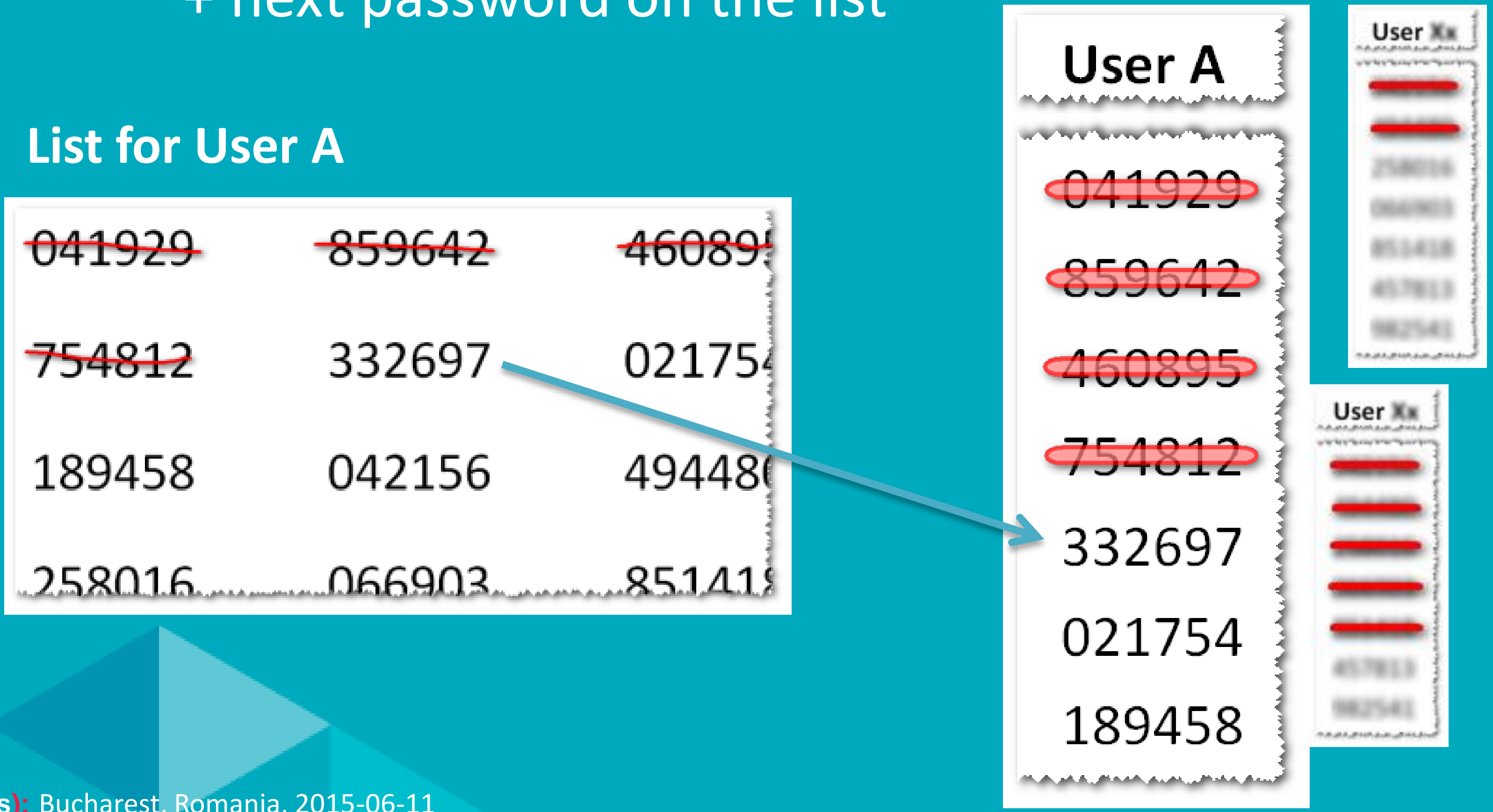
~~876287~~	~~974038~~	~~481602~~	~~035301~~
~~352756~~	386158	035698	327666
469047	115213	724823	265578
579111	155339	690403	838079
500087	353187	451550	700562
836369	435146	641900	999371

Passwords list usage

- Login = username
  + secret PIN
  + next password on the list

List for User A

Lists on the server



~~041929~~	~~859642~~	~~46089~~
~~754812~~	332697	02175
189458	042156	49448
258016	066903	85141

User A

~~041929~~

~~859642~~

~~460895~~

~~754812~~

332697

021754

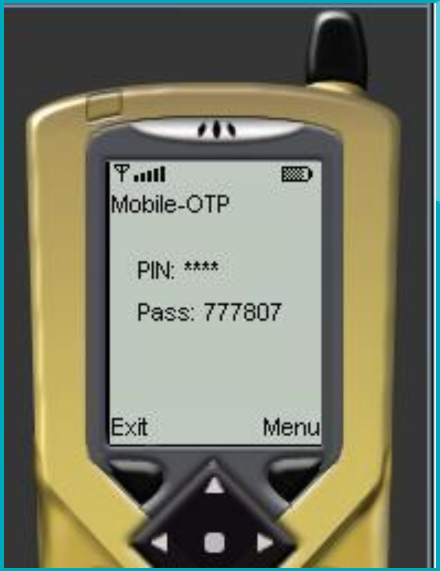
189458

Historical market leader

- Time-based automatic generator with a secret algorithm
  – 70% of the market in 2003
  (25 mio of devices have been sold up to 2003)

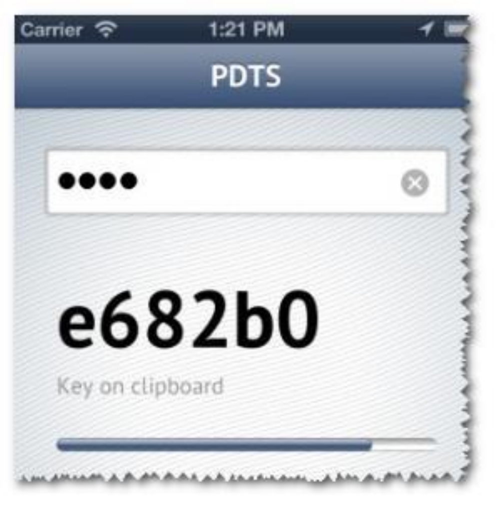
First open-source one-time password solution

- Mobile-OTP (2003)
  - Hash (md5) of a “PIN code + time based algorithm”
  - open source, more than 40 different implementations
  - Java J2ME for mobile phones
  - Unix shell script on server side


Mobile-OTP

PIN: ****

Pass: 777807



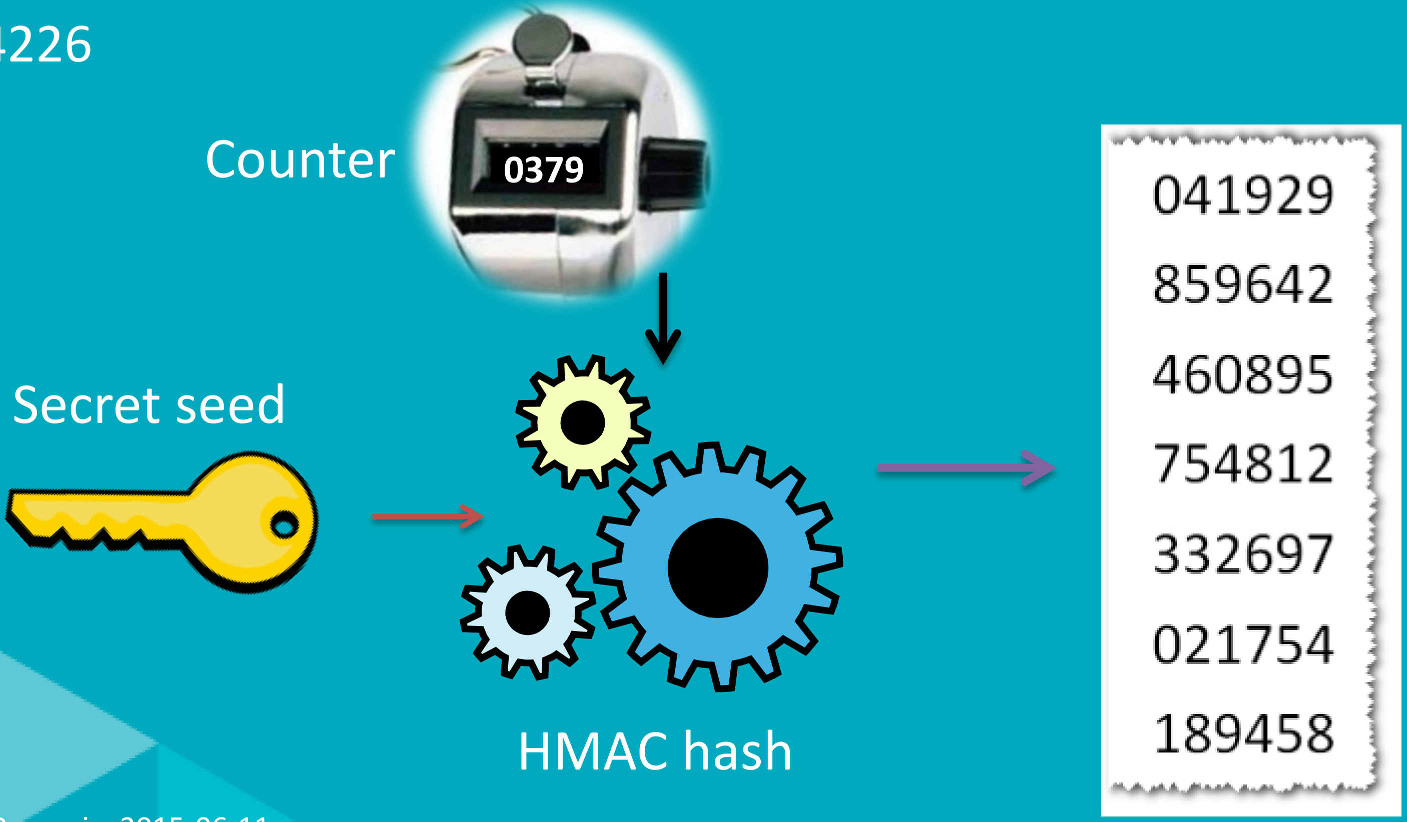
••••

e682b0

Key on clipboard

Standardized one-time password generator

- HOTP : HMAC-based One-time Password Algorithm (2005)
  - code construction is based on a HMAC hash function
  - open standard (OATH: Initiative for open authentication)
  - RFC 4226


Counter

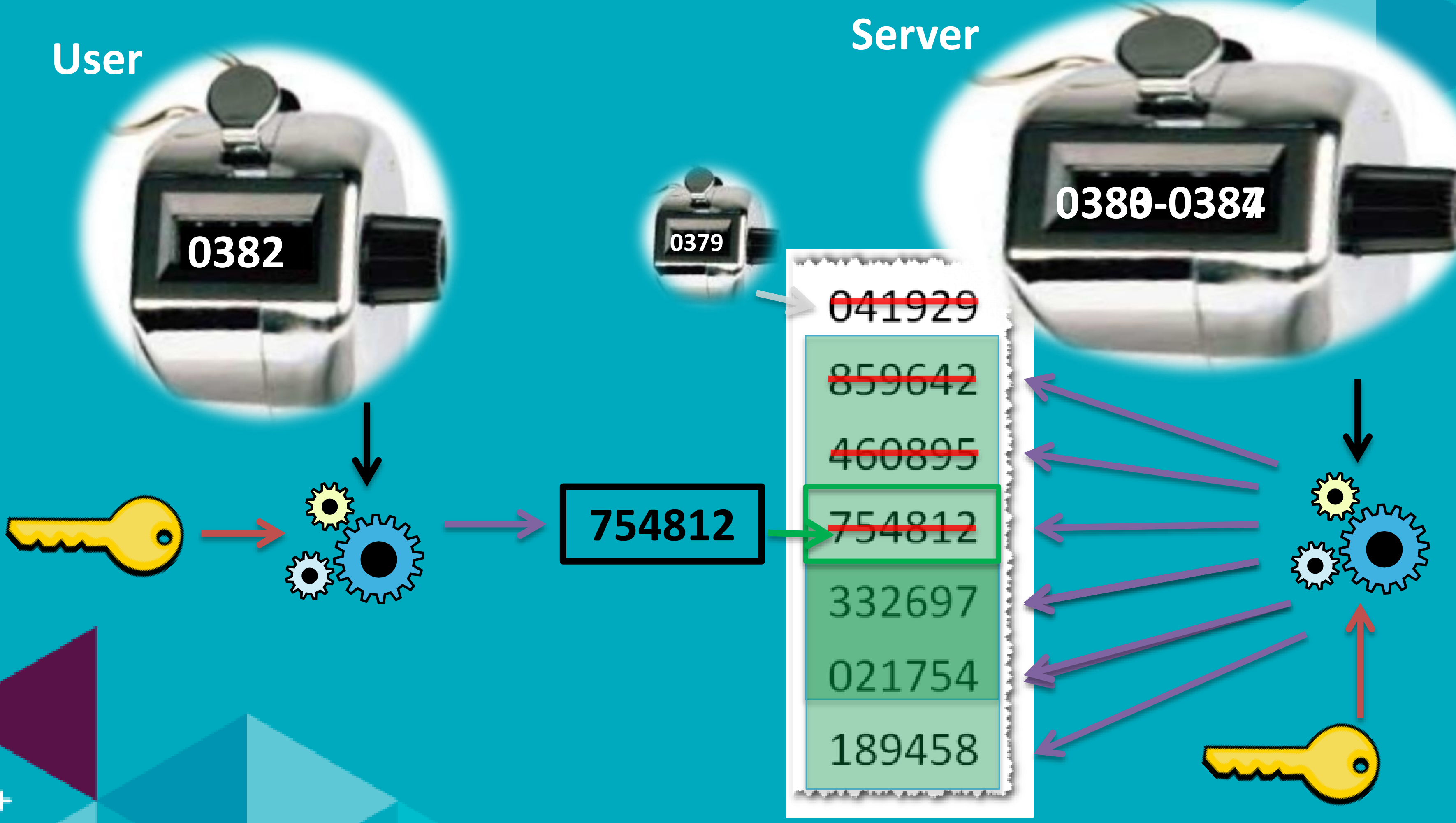
0379

Secret seed

HMAC hash

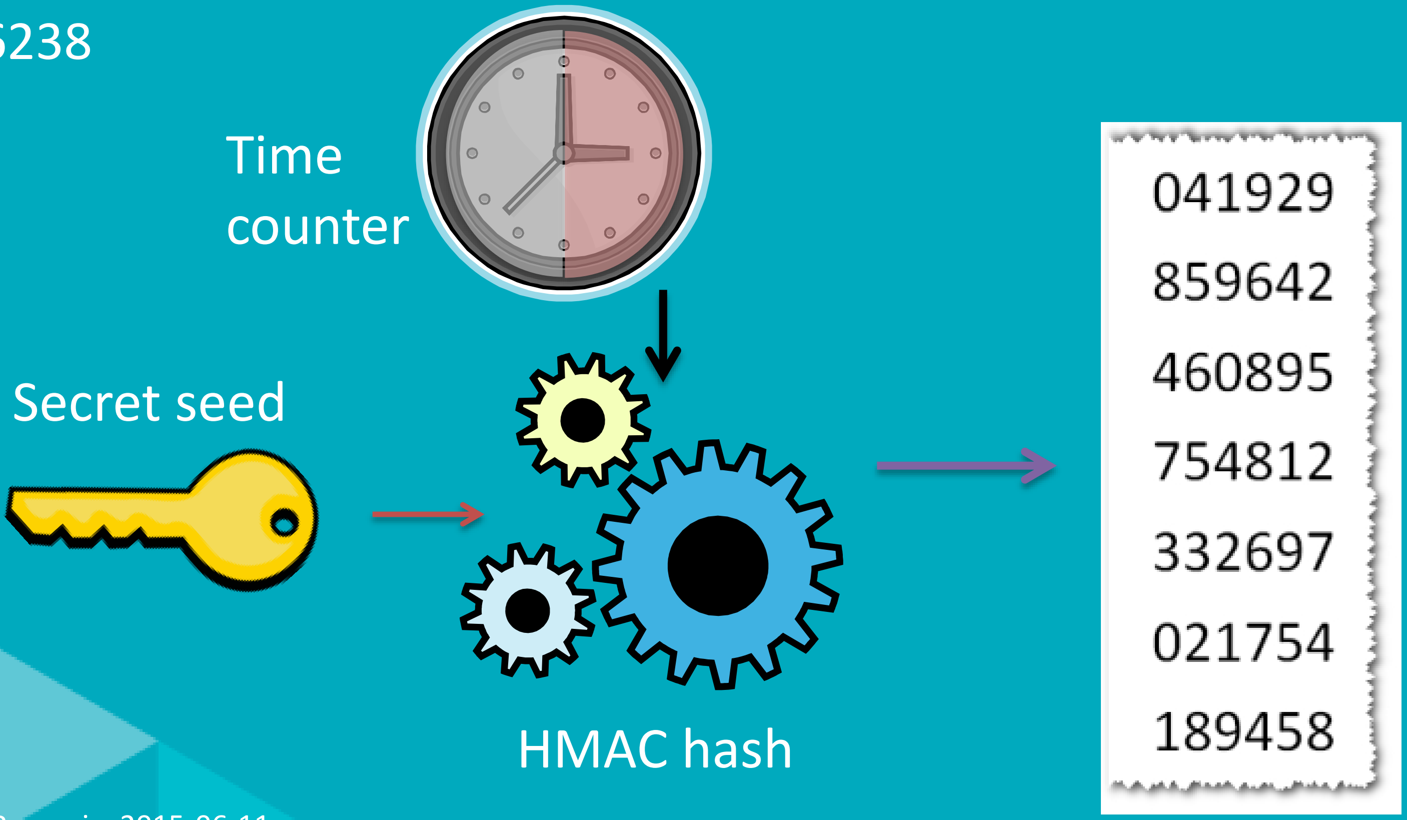
041929
859642
460895
754812
332697
021754
189458

HOTP authentication mechanism



No synchronization problem anymore with TOTP

- TOTP : Time-based One-time Password Algorithm (2008)
  - based on HOTP
  - The counter is now the time divided in slices of 30 seconds
  - RFC 6238

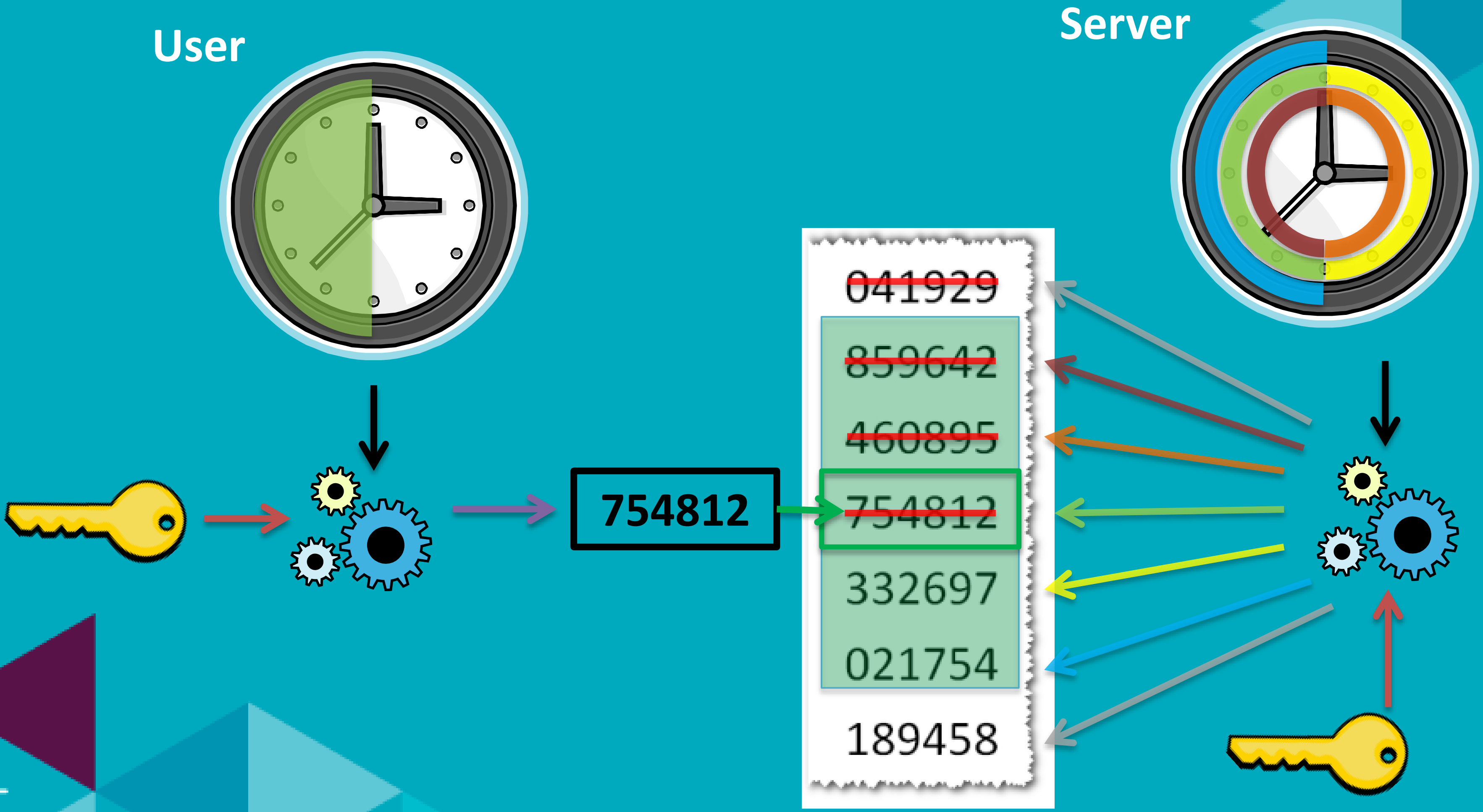


Time counter

Secret seed

HMAC hash

TOTP authentication mechanism



User

Server

754812

~~041929~~

~~859642~~

~~460895~~

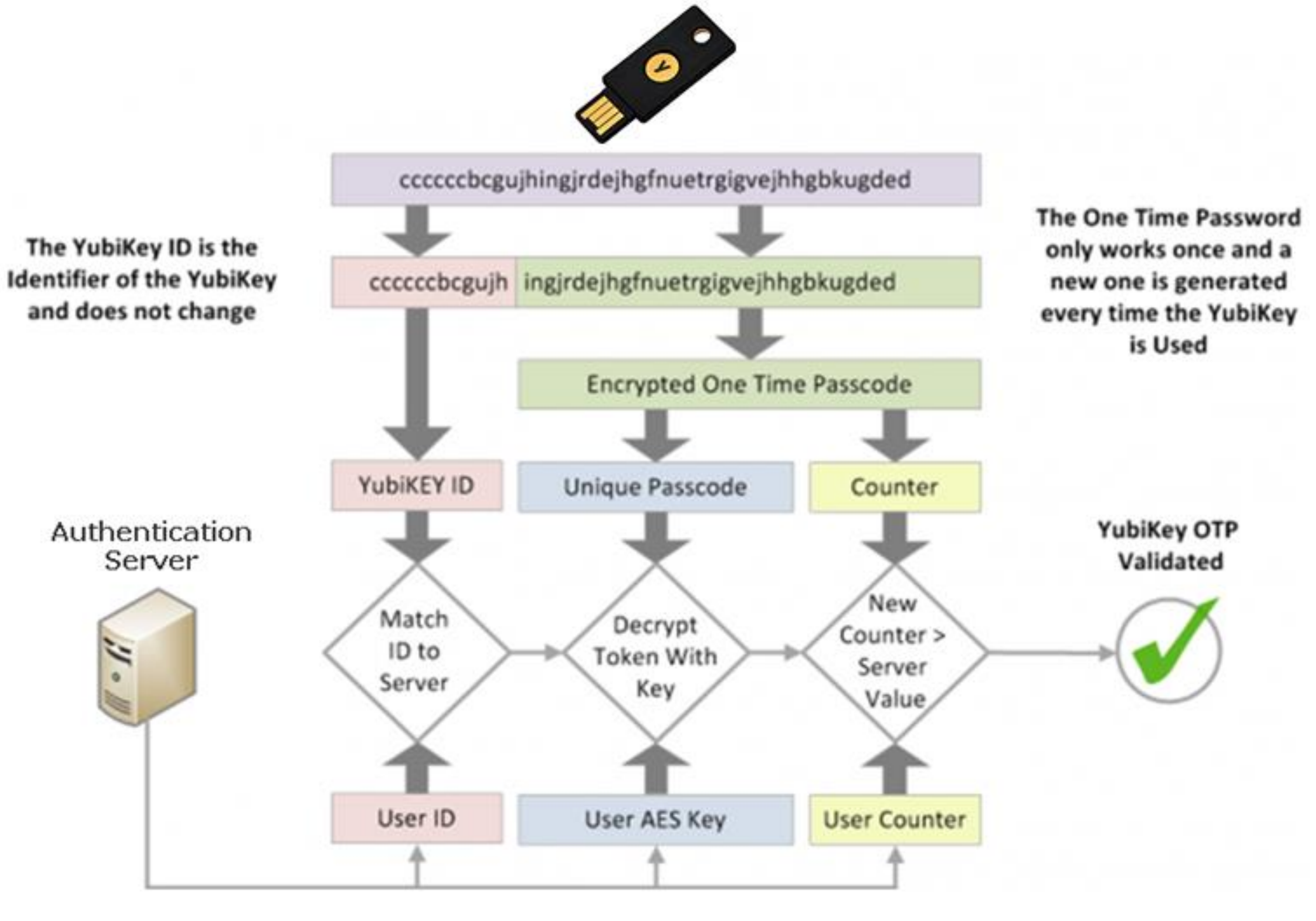
~~754812~~

332697

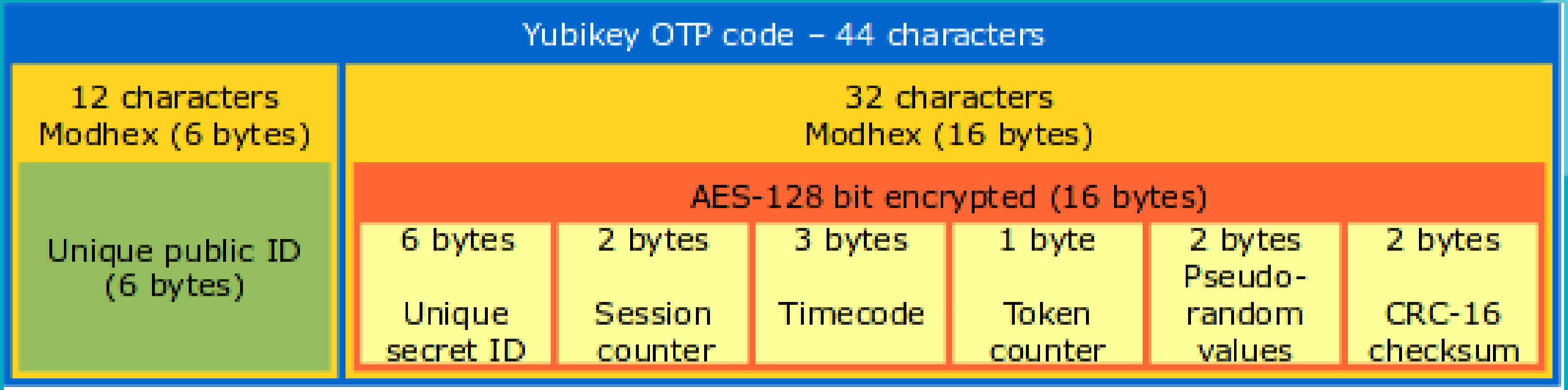
021754

189458

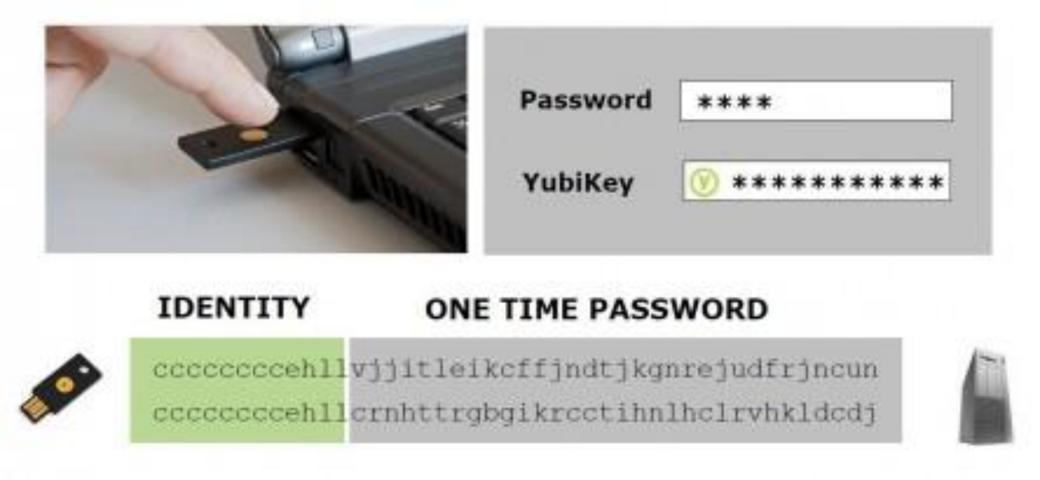
Yubico OTP


cccccbcgujhingjrdejhgfnuetrgigvejhhgbkugded
The YubiKey ID is the Identifier of the YubiKey and does not change
cccccbcgujh
ingjrdejhgfnuetrgigvejhhgbkugded
The One Time Password only works once and a new one is generated every time the YubiKey is Used
Encrypted One Time Passcode
YubiKEY ID
Unique Passcode
Counter
Authentication Server
YubiKey OTP Validated
Match ID to Server
Decrypt Token With Key
New Counter > Server Value
User ID
User AES Key
User Counter

Yubico OTP code



Yubikey OTP code – 44 characters						
12 characters Modhex (6 bytes)	32 characters Modhex (16 bytes)					
	AES-128 bit encrypted (16 bytes)					
Unique public ID (6 bytes)	6 bytes Unique secret ID	2 bytes Session counter	3 bytes Timecode	1 byte Token counter	2 bytes Pseudo-random values	2 bytes CRC-16 checksum



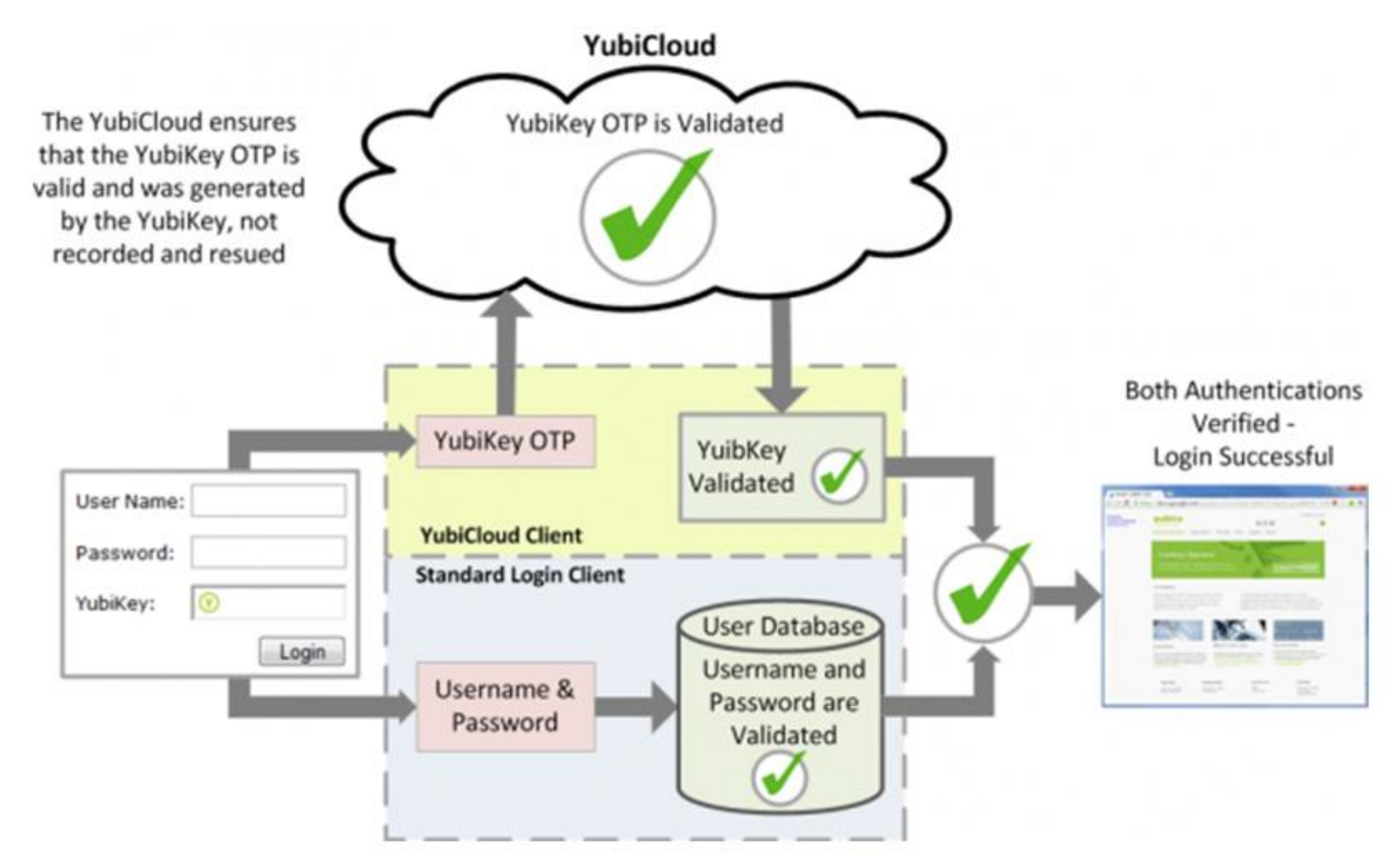
Password ****

YubiKey ***********

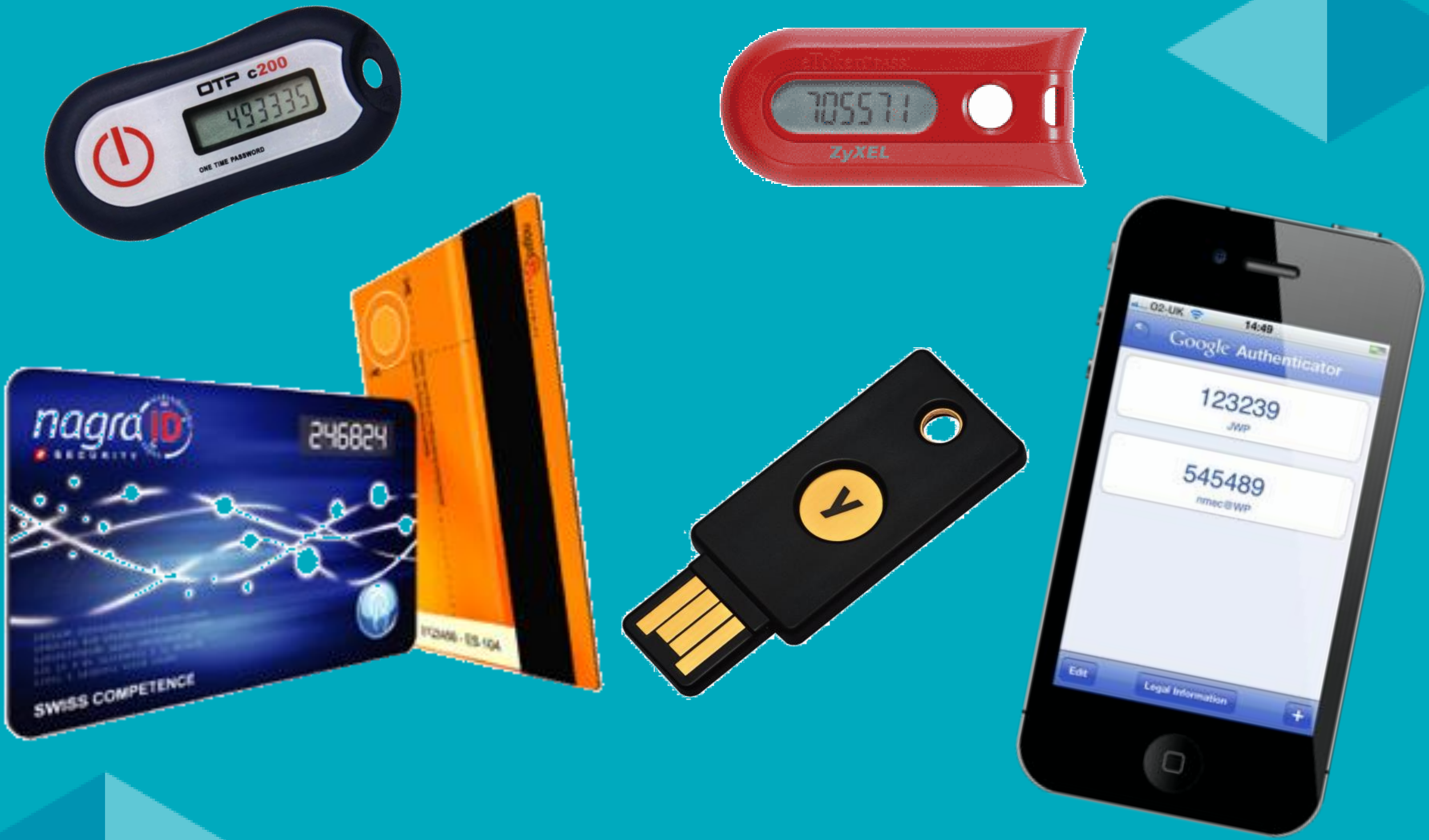
IDENTITY ONE TIME PASSWORD

```
cccccccccehllvjjitleikcffjndtjkgnrejudfrjncun
cccccccccehllcrnhttrgbgikrcctihnlhclrvhkldcdj
```

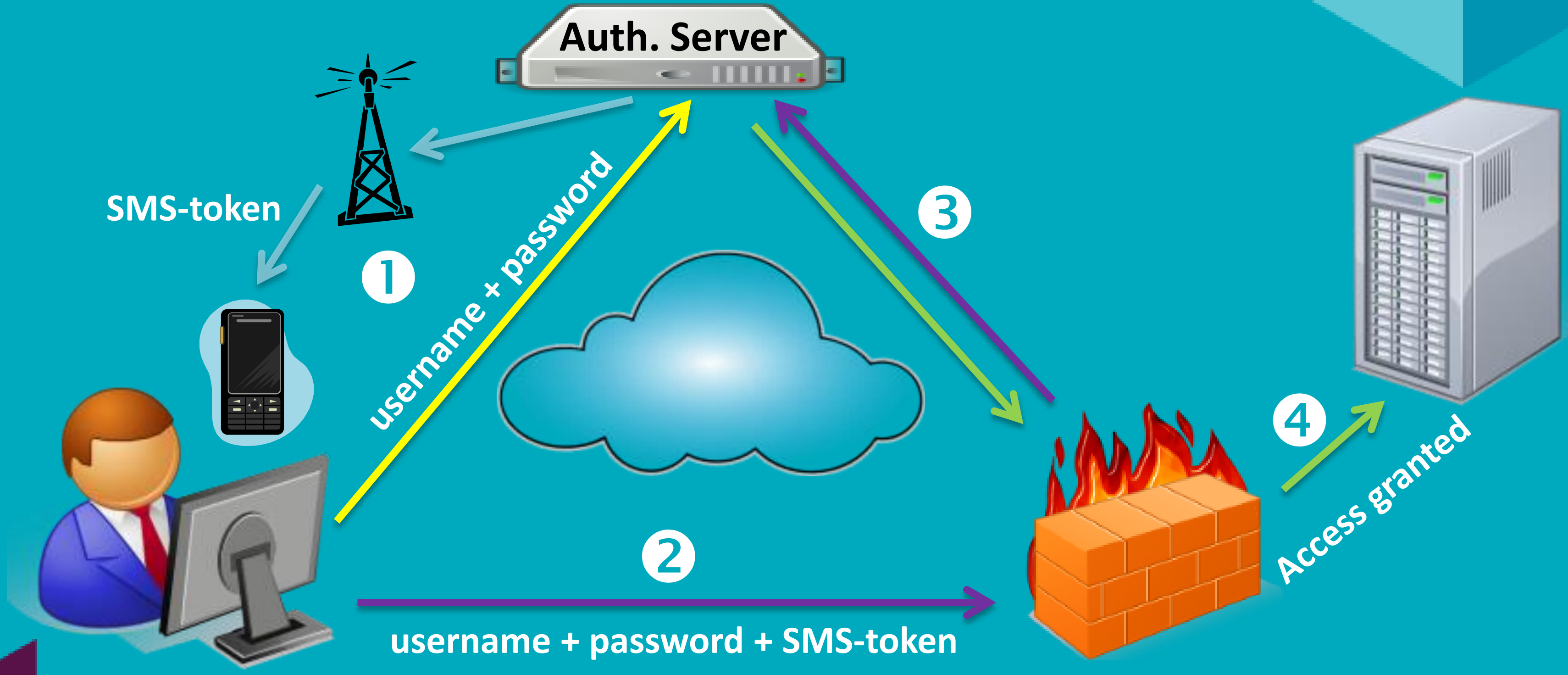
YubiCloud


YubiCloud
The YubiCloud ensures that the YubiKey OTP is valid and was generated by the YubiKey, not recorded and resued
YubiKey OTP is Validated
User Name:
Password:
YubiKey:
Login
YubiKey OTP
YuibKey Validated
YubiCloud Client
Standard Login Client
Username & Password
User Database
Username and Password are Validated
Both Authentications Verified -
Login Successful

Some HOTP and TOTP tokens



SMS-token


Auth. Server
SMS-token
1
username + password
3
2
username + password + SMS-token
4
Access granted

multi*OTP* - A PHP OPEN SOURCE LIBRARY SOLUTION

History of the **multi*OTP*** package

- 2009 PHP PoC implementing the Mobile-OTP protocol
- 2010 class creation with basic TOTP/HOTP
- 2011 Workshop during ASFWS 2011 (Application Security Forum)
- 2012 Wider deployment in the community and feedbacks
- 2013 New functionalities
  - SMS tokens
  - scratch passwords list
  - QRcode/URL provisioning
  - Client/server implementation with local cache
  - MySQL backend support

History of the **multi*OTP*** package /2

- 2014 Certification and more functionalities
  - OATH certified
  - Yubico OTP support (YubiKey)
  - Active Directory and LDAP synchronization
  - Support for Active Directory / LDAP passwords (instead of PIN)
  - First Raspberry Pi implementation
- 2015 Enhancements
  - More options based on users feedback
  - Better performance on Raspberry Pi with special proxy
  - More AD / LDAP fields support
  - Web GUI enhancements

multi*OTP*

- Why did we develop the **multi*OTP*** package ?
  - no free and easy to use solution for small companies
  - a lot of existing commercial products need Windows Server
  - Existing products need a lot of resources
- Why open source ?
  - To receive feedbacks and proposals from the users
  - security issues are analyzed by other developers
  - users can be sure that there is no Trojan and other NSA-friendly “tools” in our code

multi*OTP* concept

- open source PHP class (embedded in only one file)
  - OS independent
  - Works also on any web server, including in shared hosting
- data or stored in flat files or in a MySQL database
- all methods are implemented in a command line tool
  - Command line tool is compatible with the centralized open source authentication server FreeRADIUS
  - The system administrator can create scripts in order to handle the package and to create users

multi*OTP* concept (2)

- common standards are supported
  - Mobile-OTP, HOTP, TOTP, Yubico OTP
  - SMS tokens
  - scratch passwords list
- simple web GUI for all common tasks (since 2014)
- HOTP and TOTP software tokens can simply be configured by flashing a QRcode generated by multiOTP
- hardware tokens definition files can be imported
  - some proprietary files are supported (Authenex or SafeNet definition files)
  - any standard PSKC files (since December 2013)
  - Yubico log file in Traditional format (since November 2014)

multi*OTP* library
website integration in 4 lines !

- require_once('multiotp.class.php');
- $multiotp = new Multiotp('MyPersonalEncryptionKey'); *
  $multiotp->SetUser($user);
- $result = $multiotp->CheckToken($tokens);

multi*OTP* package can be installed on Windows

- RADIUS authenticator installed in 3 minutes !
- surf on http://www.**multi*OTP***.net
- download the last version
- unpack the files in the **C:\multiotp\** folder
- read the readme file ;-)
- install the FreeRADIUS service
  - **C:\multiotp\radius_install.cmd**
- that’s it !

multi*OTP*
How to create a user

- create the user on the server side

  ```
  C:\multiotp>multiotp -fastcreate devtalks
  11 INFO: User successfully created or updated
  ```

- save the QRcode image in a file

  ```
  C:\multiotp>multiotp -qrcode devtalks C:\multiotp\devtalks.png
  16 INFO: QRcode successfully created
  ```

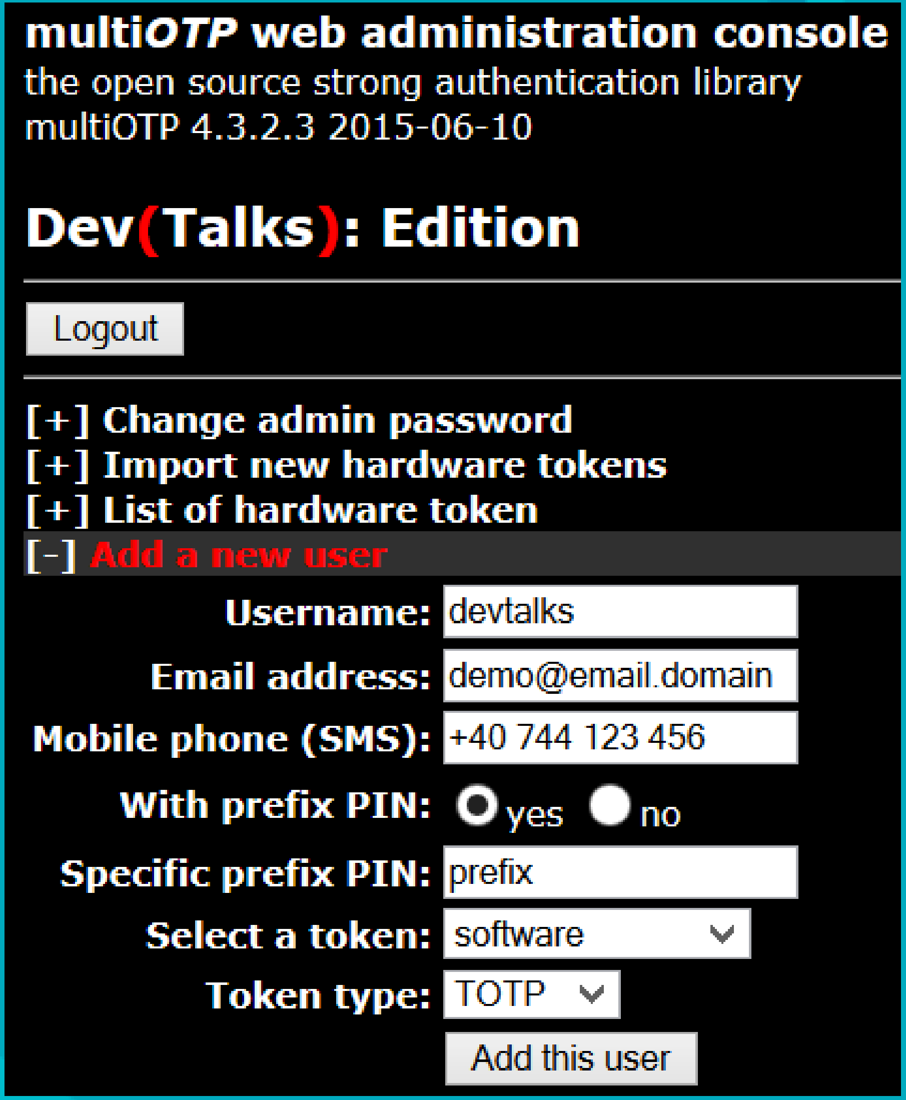
- Send the QRcode to the user

  (using a secure channel !)

- **… or simply use the web interface to create a user**

  and print a nice HTML provisioning page;-) !

multi*OTP* simple web GUI



multi*OTP* web administration console

the open source strong authentication library

multiOTP 4.3.2.3 2015-06-10

Dev(Talks): Edition

[+] Change admin password

[+] Import new hardware tokens

[+] List of hardware token

[-] Add a new user

Username: devtalks

Email address: demo@email.domain

Mobile phone (SMS): +40 744 123 456

With prefix PIN: ● yes ○ no

Specific prefix PIN: prefix

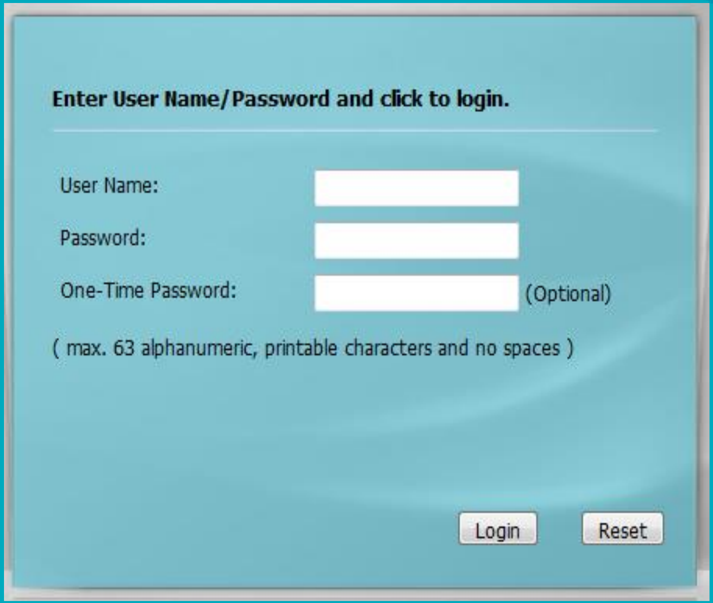
Select a token: software

Token type: TOTP

multi*OTP*
easy QRcode provisioning

Flash it with Google Authenticator App !

multi*OTP*
Typical usage


Enter User Name/Password and click to login.

User Name:

Password:

One-Time Password: (Optional)

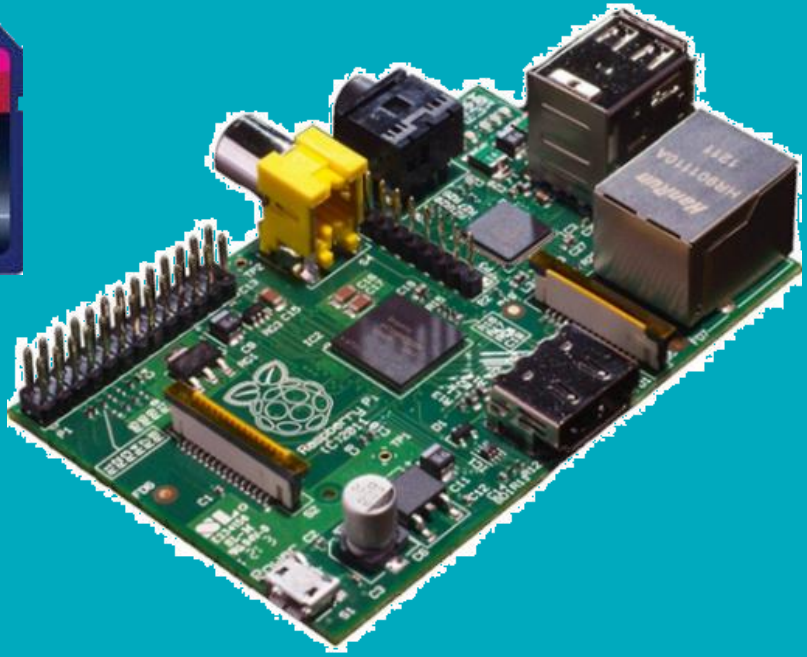
(max. 63 alphanumeric, printable characters and no spaces)

devtalks

HOW TO SETUP AN AUTHENTICATION DEVICE FOR LESS THAN $100 ?

Hardware selection

- Raspberry Pi
  - – very cheap (< $ 40)
  - – no OS licence (Debian Linux or others)
  - – widely distributed
  - – community support
  - – microUSB powered
  - – CPU 700 MHz (ARM)
  - – RAM 512 MB



How to make your own strong authentication server ?

SD card with Debian Linux for Raspberry Pi ($10)

+ **multi*OTP*** ($

Raspberry Pi enclosure ($10)

80

5V power supply ($10)

Real-time clock ($15)

Raspberry Pi ($35)

LIVE-DEMO WITH multi*OTP* INSTALLED ON A Raspberry Pi

Dev(Talks): Bucharest, Romania

2015-06-11

Thanks for your attention !

André Liechti
SysCo systèmes de communication sa

www.**multi*OTP***.net
slidehare.net/multiotp

@andreliechti
@multiotp

oath
initiative for open authentication
CERTIFIED