DEVCON

LIFERAY DEVELOPER CONFERENCE

LIFERAY

Liferay and Google Authenticator integration to deliver two factor authentication

Rafik HARABI

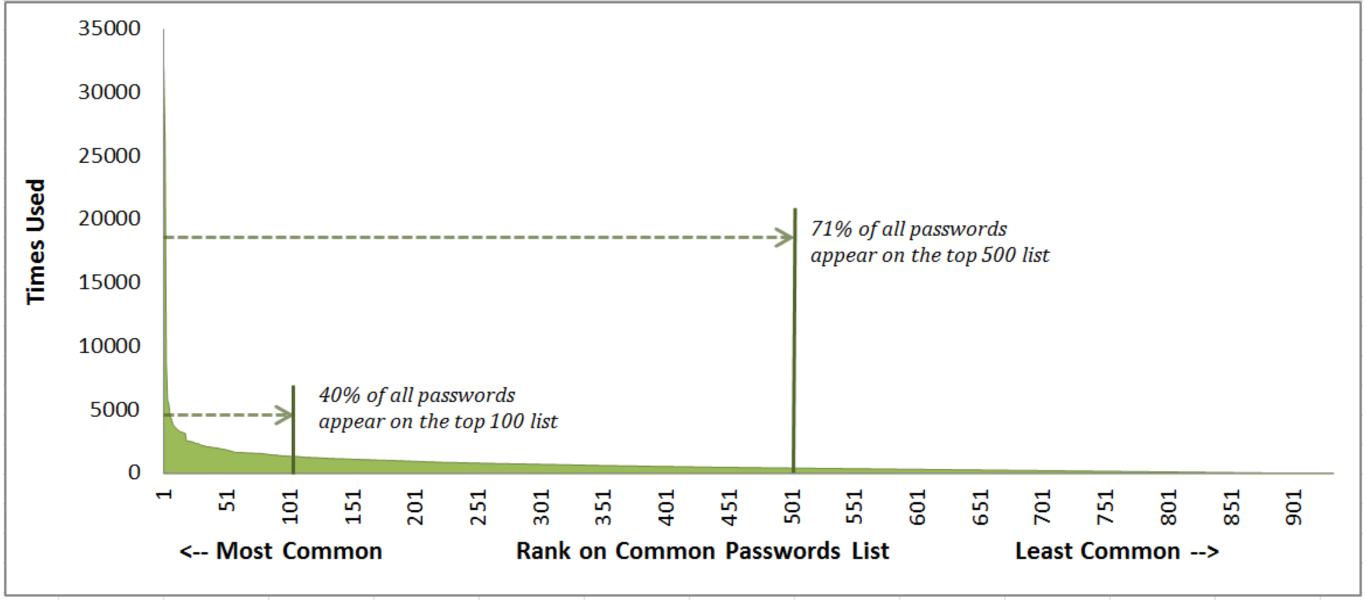
Enterprise Portal Consultant

Agenda

- Introduction
- Brief overview of TOTP algorithm
- Two-factor authentication integration: the technical solution
- Demo
- Conclusion
- Q & A

Introduction

- Why two-factor authentication ?
  - Authentication based attacks are using in 4 out of 5 attacks.
  - Password leaks:
    - Captured, Phished, Cracked, Sniffed, Stolen, Guessed ….



Source: https://xato.net/passwords/more-top-worst-passwords/(Mark Burnett)

Introduction

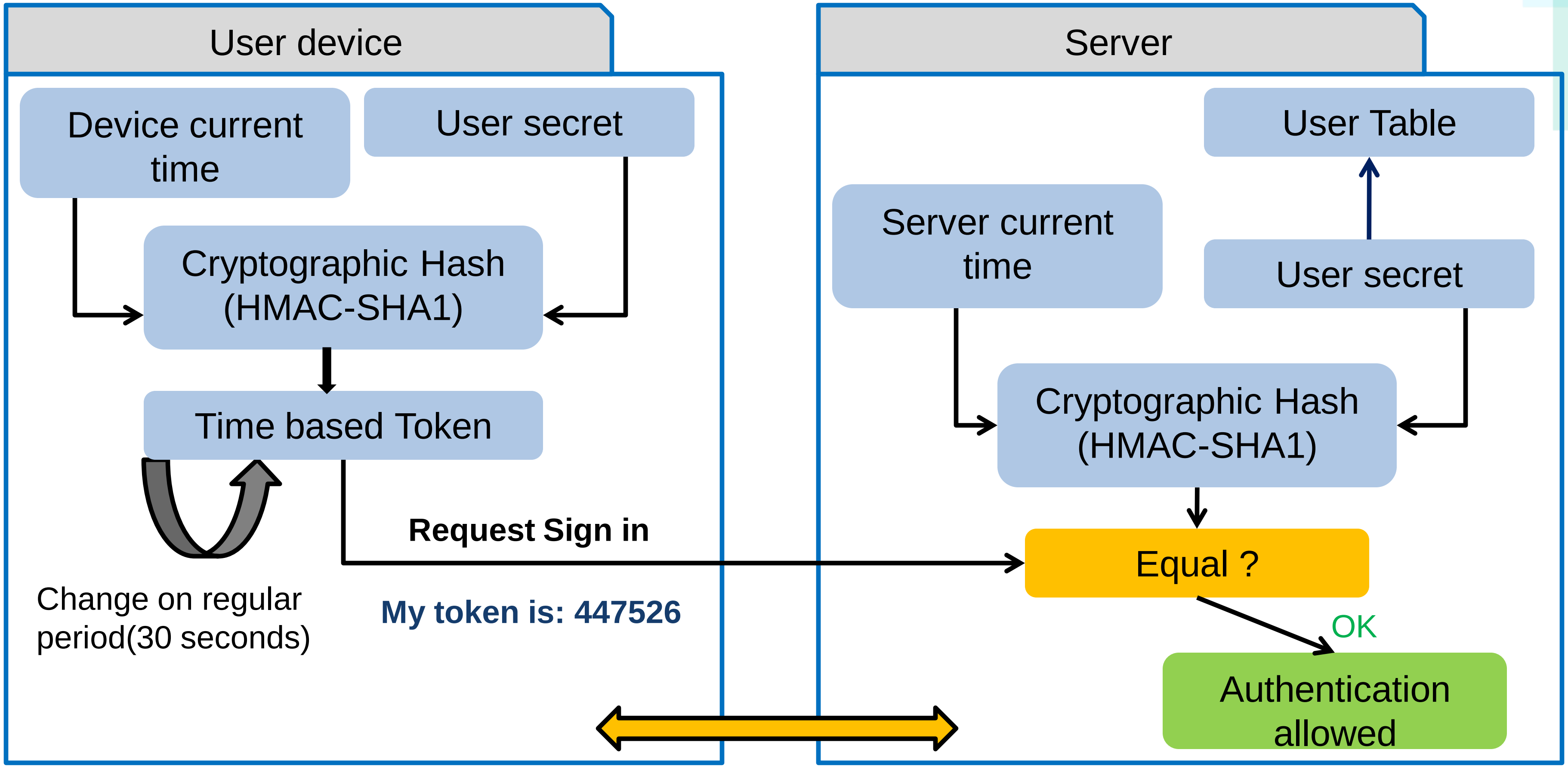
- Strengthen authentication:
    - Require a second factor after the username/password stage

- Why Google Authenticator ?
    - Easy to install (no special configuration needed)
        - android, iOS and blackberry.
    - Open source (helpfull technical integration)
    - Reduce TCO :
        - avoid custom implementation
        - reduce deployment and training costs
    - Improve end user experience: installed on device that people already have, know how to use.

Brief overview of TOTP algorithm

- TOTP: Time-based One-time Password Algorithm
- Specified by IETF under RFC 6238 on May 2011.
- Open and known: a reference implementation is provided with the RFC.
- Generated TOTP tokens are based on:
  - A shared key : saved on the server and associated to the user account on Google Authenticator.
  - A moving factor: the current time
  - .

TOTP algorithm: How it works

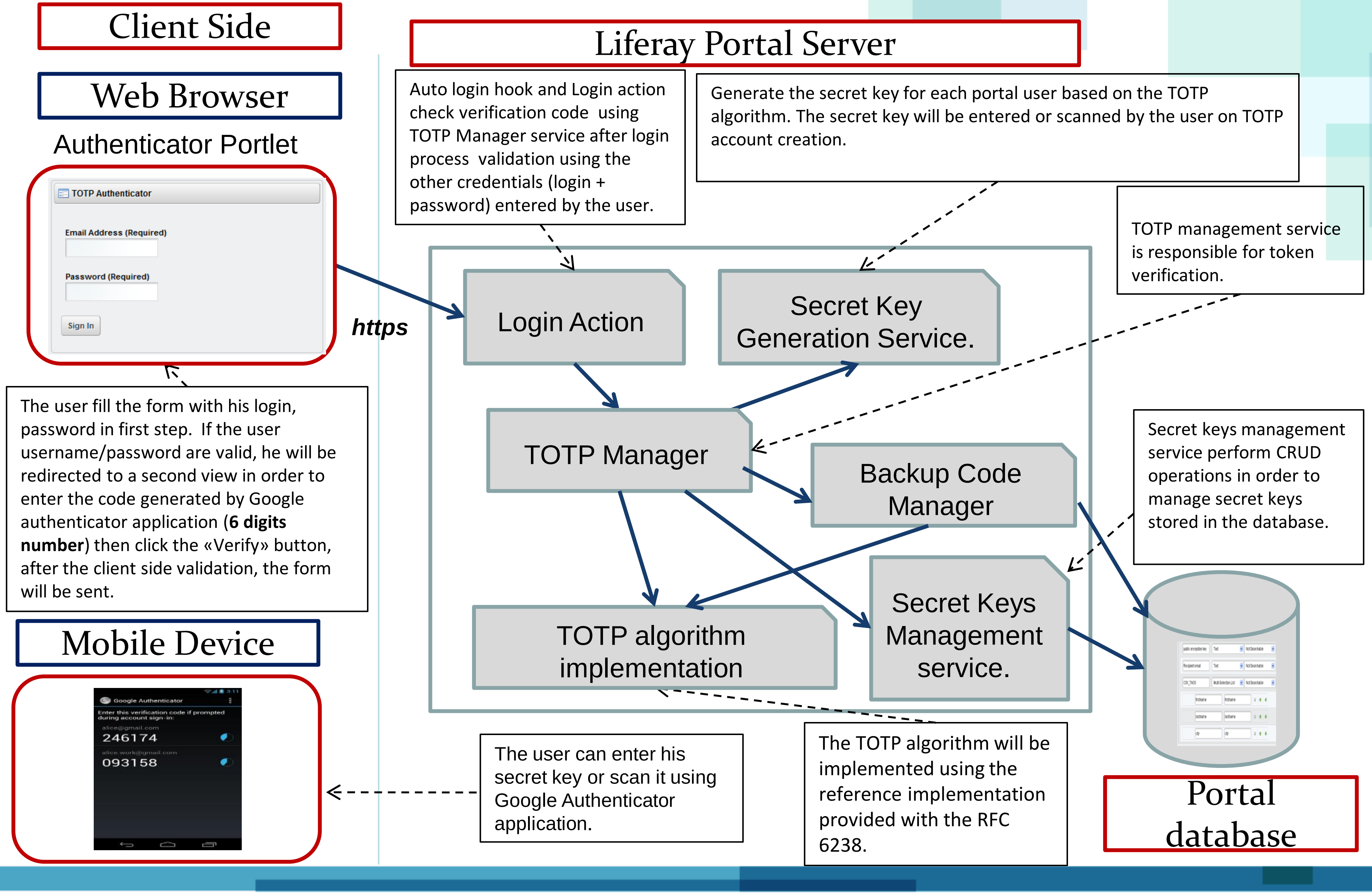


Clocks should be synchronized

TOTP algorithm: How it works

- What you should keep in mind:
  - The TOTP uses a shared secret and the current time to calculate a code, which is displayed for the user and regenerated at regular intervals.
  - Because the token and the authentication server are disconnected from each other, the clocks of each must be perfectly in sync.

Technical solutions overview



Client Side

Web Browser

Authenticator Portlet

https

The user fill the form with his login, password in first step. If the user username/password are valid, he will be redirected to a second view in order to enter the code generated by Google authenticator application (**6 digits number**) then click the «Verify» button, after the client side validation, the form will be sent.

Mobile Device

The user can enter his secret key or scan it using Google Authenticator application.

Liferay Portal Server

Auto login hook and Login action check verification code using TOTP Manager service after login process validation using the other credentials (login + password) entered by the user.

Generate the secret key for each portal user based on the TOTP algorithm. The secret key will be entered or scanned by the user on TOTP account creation.

TOTP management service is responsible for token verification.

Secret keys management service perform CRUD operations in order to manage secret keys stored in the database.

Login Action
Secret Key Generation Service.
TOTP Manager
Backup Code Manager
Secret Keys Management service.
TOTP algorithm implementation

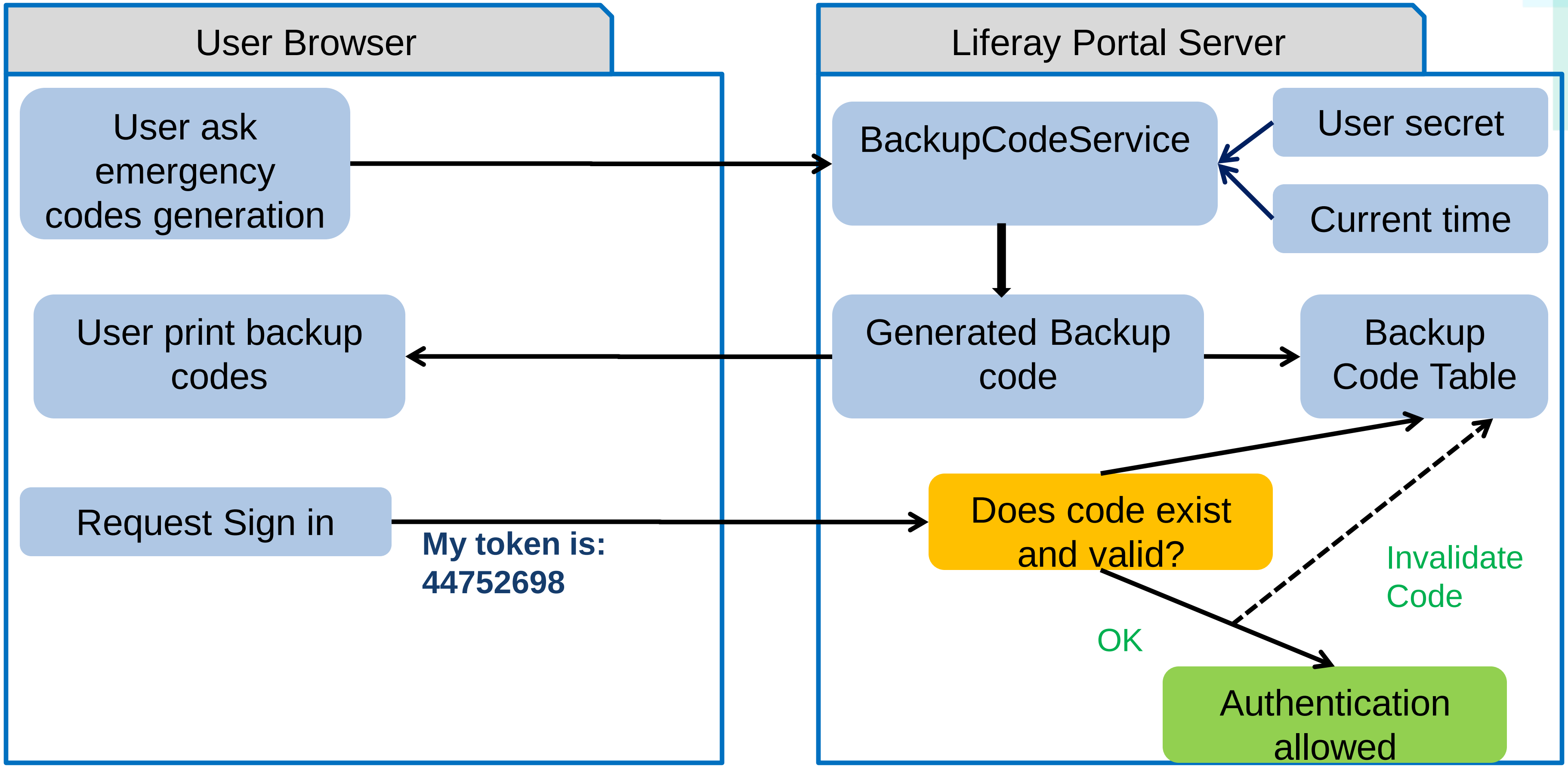
The TOTP algorithm will be implemented using the reference implementation provided with the RFC 6238.

Portal database

Technical Solution

- Generate TOTP token:
  - 6 digits number generated on regular intervall on Google Authenticator mobile application by combining user secret key and the current time.
  - On Liferay server, it will be generated only on demand.
- Validate TOTP token:
  - A TOTP token will be generated by the Liferay server at the login time in order to validate TOTP received from the user.
- Generate Backup Code:
  - Emergency code generated by BackupCodeService on Liferay.

Technical Solution: emergency code



User Browser

User ask emergency codes generation

User print backup codes

Request Sign in

My token is: 44752698

Liferay Portal Server

BackupCodeService

User secret

Current time

Generated Backup code

Backup Code Table

Does code exist and valid?

Invalidate Code

OK

Authentication allowed

Technical Solution: emergency code

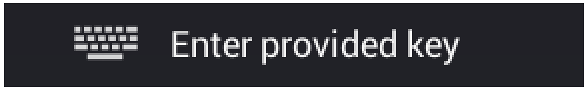
- Generated TOTP of 8 digits number:
  - Should be stored in database
  - Can be used only one time
  - Generate by a set of 10
  - Regenerated on demand
  - On regeneration, all old TOTP backup code will be invalidated.
  - Doesn’t need time synchronization

Technical Solution: user secret key

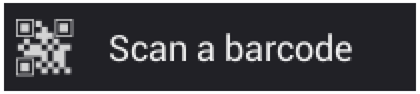
- Display user key as QR Code for Google Authenticator:
  - Better for UX:

2EBMOLPXXTZLOHSQ

VS



Enter provided key



Scan a barcode

  - Google Authenticator Key URI format:

otpauth://totp/useLabel?secret=userKey

Technical Solution: Time Sync

- Time sync between mobile devices and Liferay Portal Server:
  - All portal users are located in same time zone:
    - Synchronize your Liferay server to an NTP server.
  - Portal users are located in different time zone:
    - Use the Google Authenticator application method:
    - Synchronize to Google time.

Technical Solution: Time Sync

- Sync with Google servers time:
  - Based on Apache HttpClient :

```
private static final String URL =
"https://www.google.com";
HttpClient httpClient = new DefaultHttpClient();
HttpHead request = new HttpHead(URL);
HttpResponse httpResponse = httpClient.execute(request);
Header dateHeader = httpResponse.getLastHeader("Date");
String dateHeaderValue = dateHeader.getValue();
Date networkDate = DateUtils.parseDate(dateHeaderValue);
return networkDate.getTime();
```

  - Require full internet access

Technical Solution: Secret key encryption

- Manage secret keys:
  - Protect users keys by encrypting their:
    - Use Liferay encryption utility :

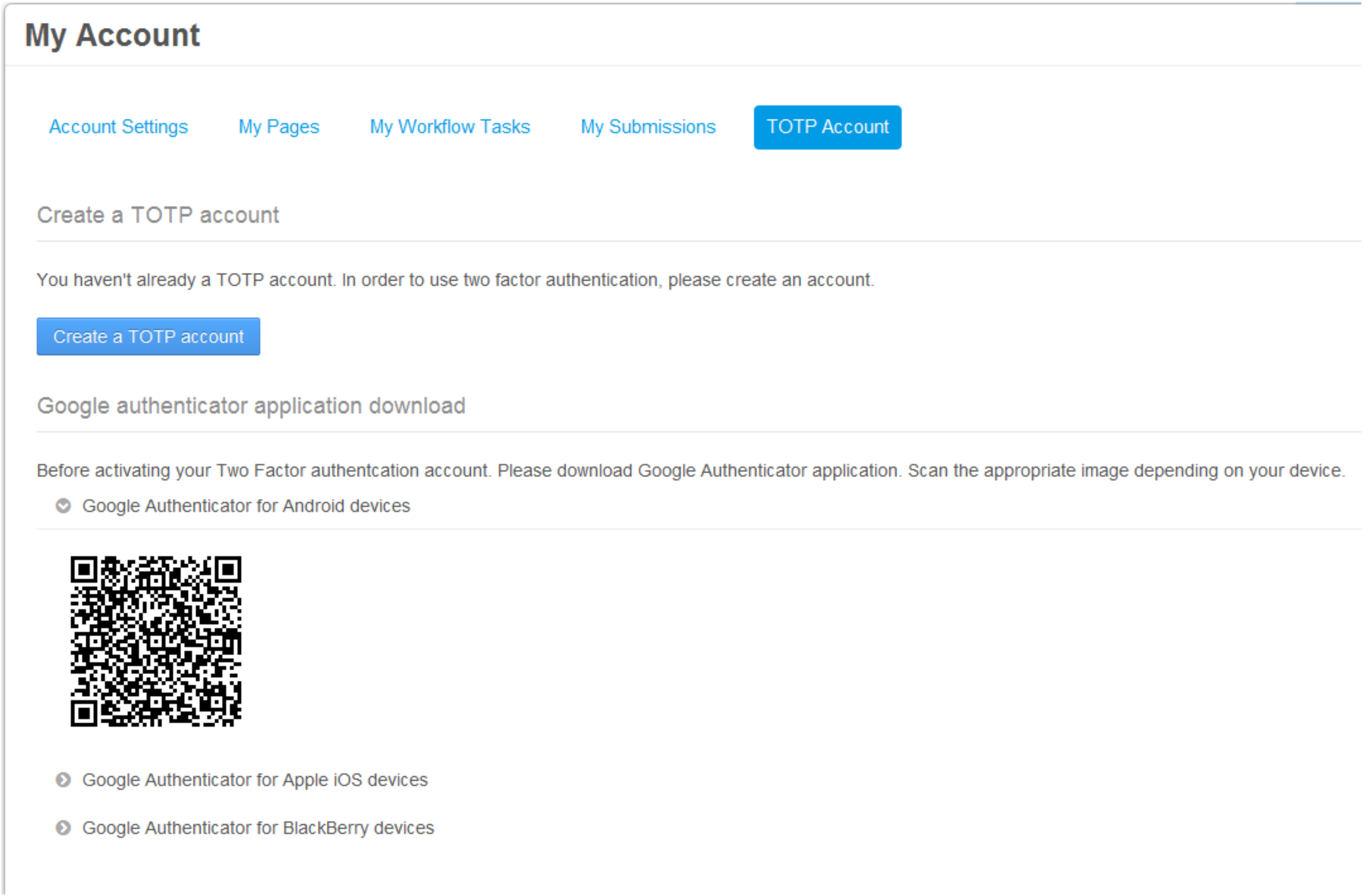
```
Encryptor.encrypt(company.getKeyObj(), plainSecretKey)
 Encryptor.decrypt(company.getKeyObj(), encryptedSecretKey)
```

  - Change encryption algorithm in portal-ext.properties

```
# Company encryption alogorithm
company.encryption.algorithm=AES
# Company encryption key size
company.encryption.key.size=128
```

Demo !

Demo



My Account

Create a TOTP account

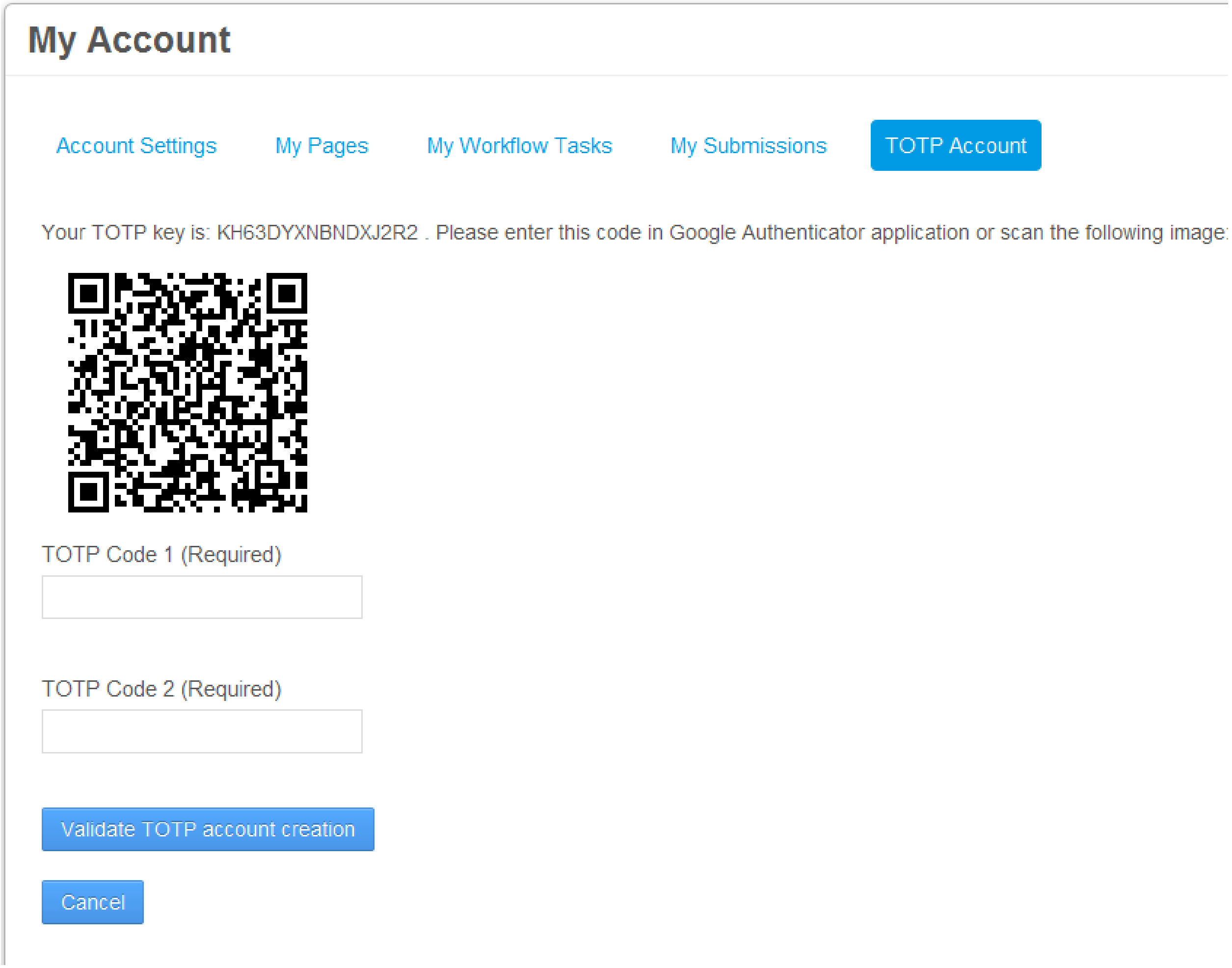
You haven't already a TOTP account. In order to use two factor authentication, please create an account.

Google authenticator application download

Before activating your Two Factor authentcation account. Please download Google Authenticator application. Scan the appropriate image depending on your device.

- Google Authenticator for Android devices
- Google Authenticator for Apple iOS devices
- Google Authenticator for BlackBerry devices

Demo

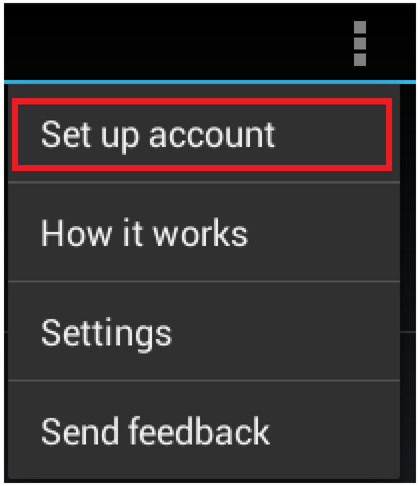


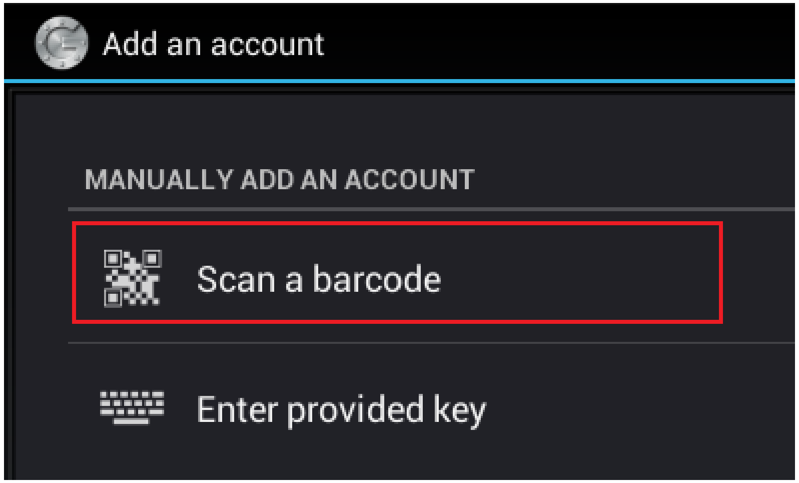
Your TOTP key is: KH63DYXNBNDXJ2R2 . Please enter this code in Google Authenticator application or scan the following image:

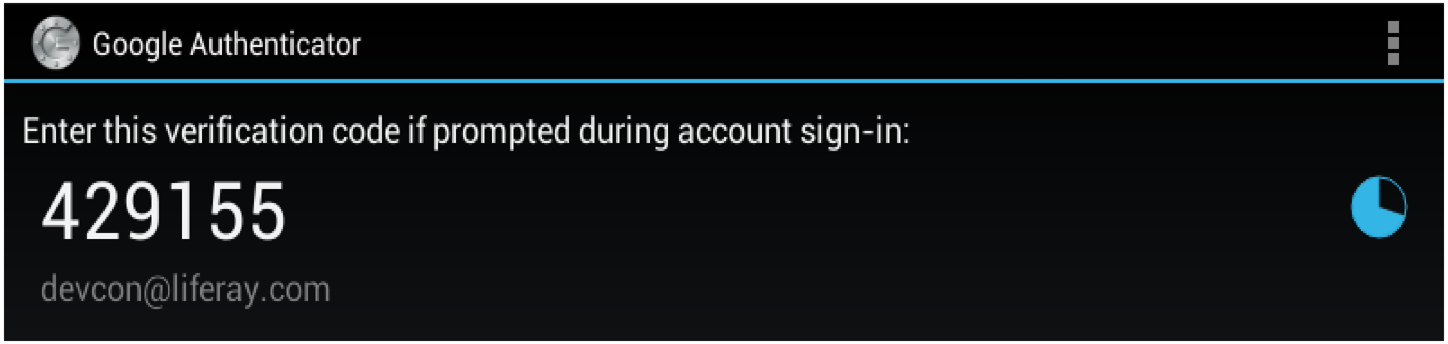
TOTP Code 1 (Required)

TOTP Code 2 (Required)

Demo





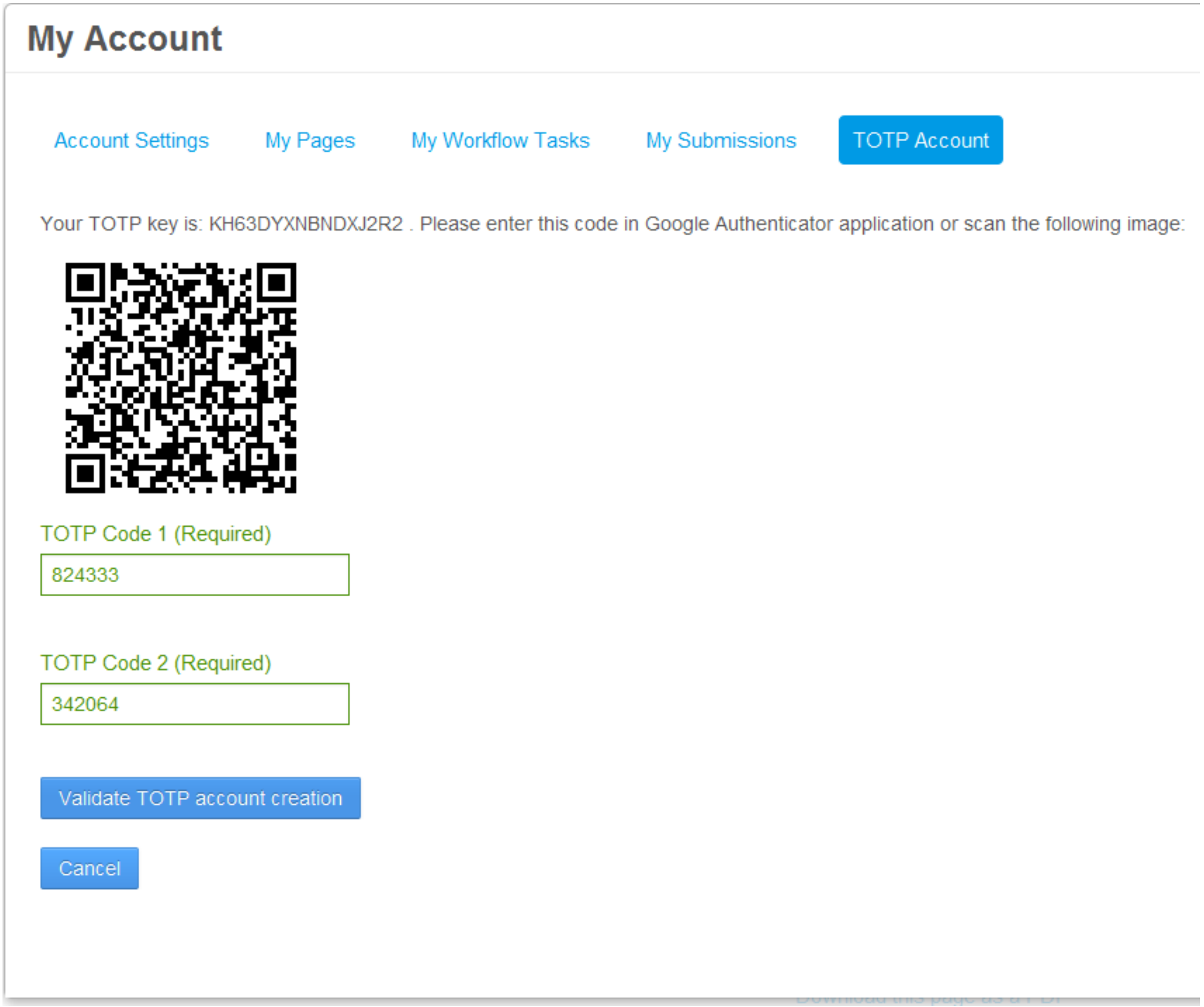


Enter this verification code if prompted during account sign-in:

429155

devcon@liferay.com

Demo



My Account

Account Settings | My Pages | My Workflow Tasks | My Submissions | TOTP Account

Your TOTP key is: KH63DYXNBNDXJ2R2 . Please enter this code in Google Authenticator application or scan the following image:

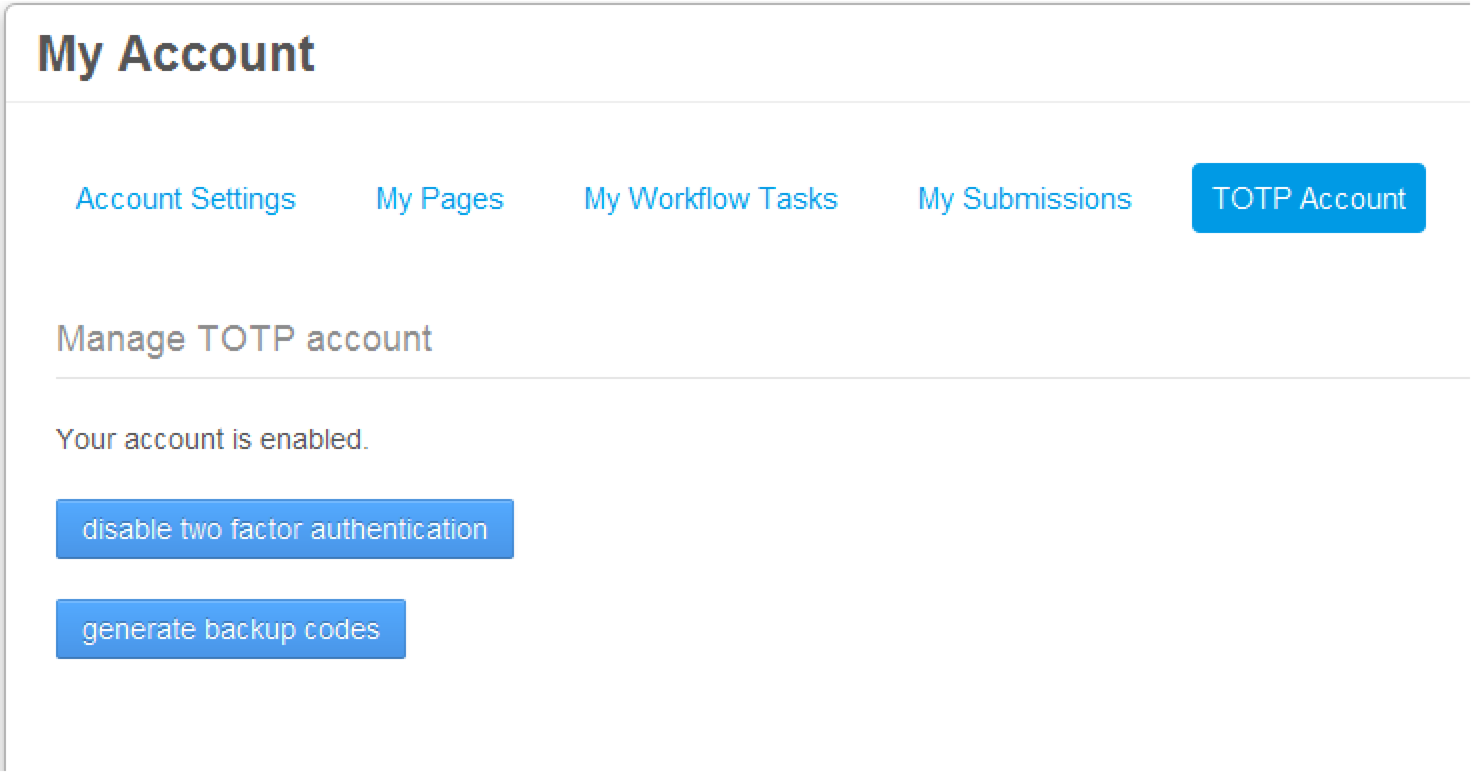
TOTP Code 1 (Required)

824333

TOTP Code 2 (Required)

342064

Demo

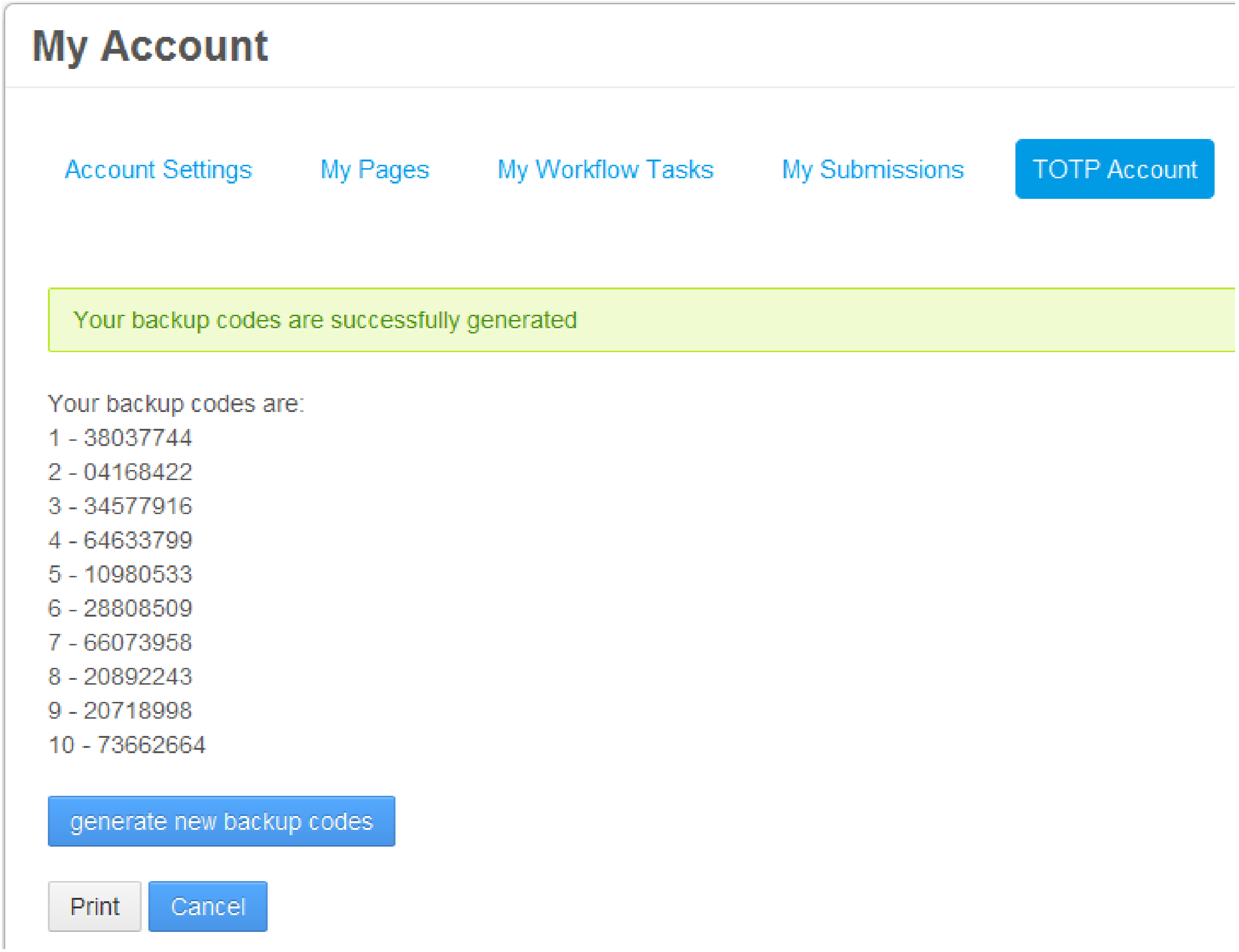


My Account

Manage TOTP account

Your account is enabled.

Demo

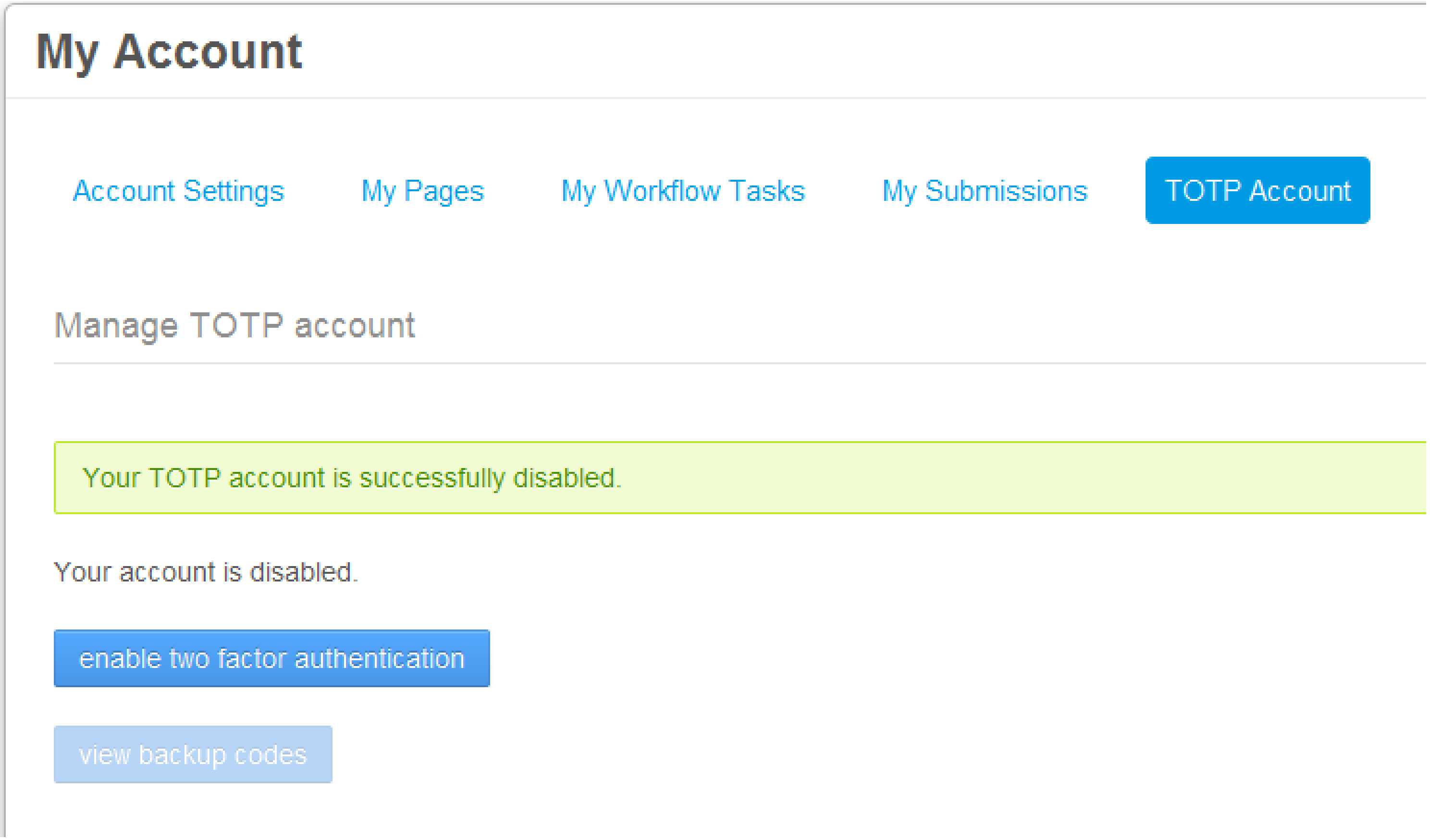


My Account

Your backup codes are successfully generated

Your backup codes are:
1 - 38037744
2 - 04168422
3 - 34577916
4 - 64633799
5 - 10980533
6 - 28808509
7 - 66073958
8 - 20892243
9 - 20718998
10 - 73662664

Demo



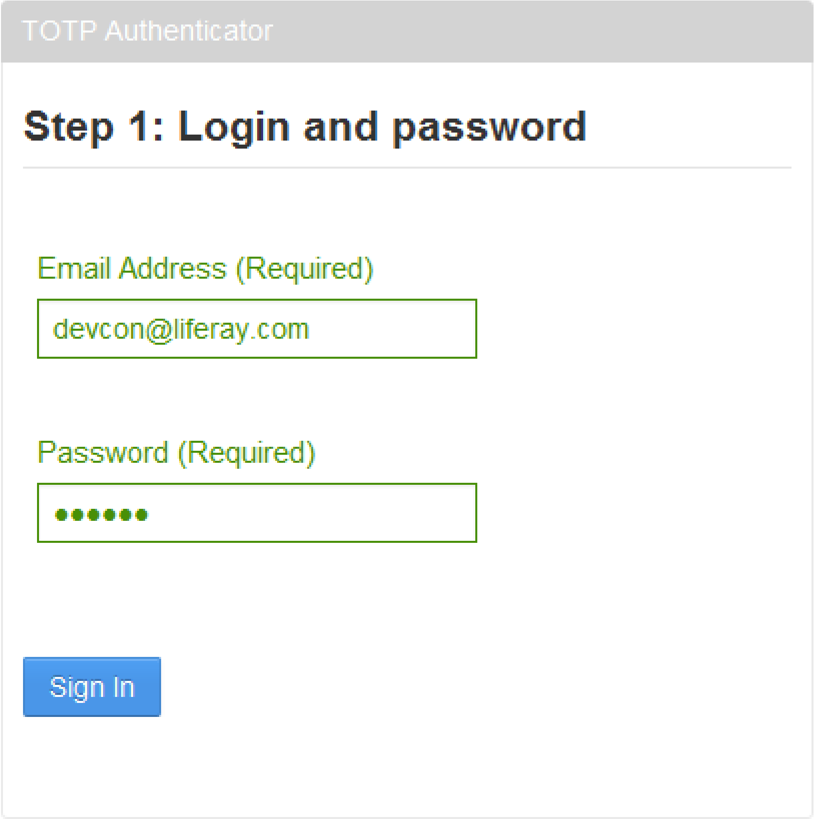
My Account

Manage TOTP account

Your TOTP account is successfully disabled.

Your account is disabled.

Demo

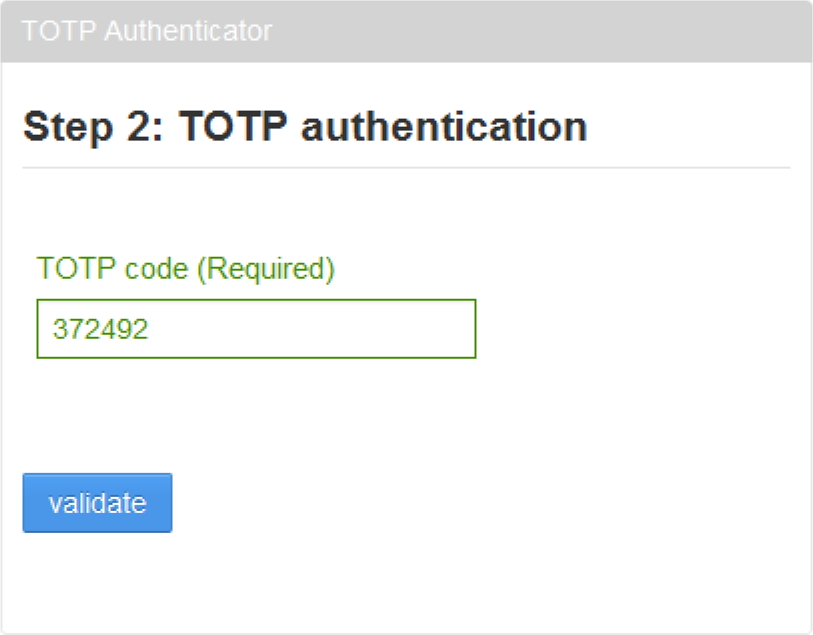


TOTP Authenticator

Step 1: Login and password

Email Address (Required): devcon@liferay.com

Password (Required): ●●●●●●



TOTP Authenticator

Step 2: TOTP authentication

TOTP code (Required): 372492

Conclusion

- Benefits:
  - 1 packaged war.
  - Easy to deploy/undeploy: doesn’t affect liferay core services and native login portlet.
  - Avoid development of a custom TOTP client.
- To improve:
  - Enhance administration capabilities‘ : enabling portal administrator to configure Totp authentication based on roles.
  - Manage Totp accounts by portal administrator.

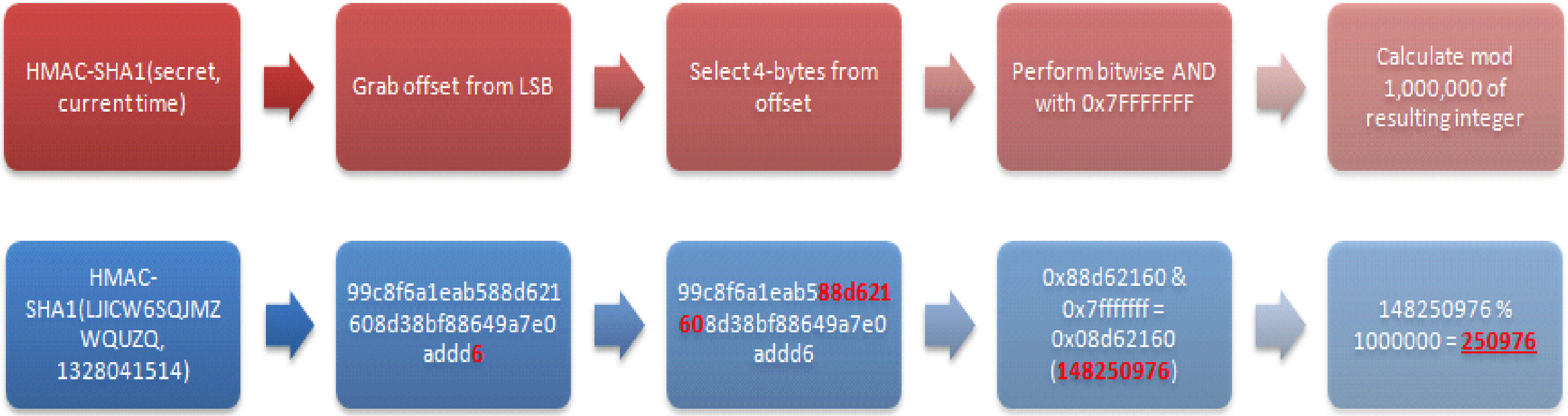
Any questions ?

- Contact:

Rafik HARABI
Enterprise Portal Consultant
Tel: +33 (6) 09 73 52 04
rafik.harabi@innovsquare.com

Appendix

- TOTP Calculation:



HMAC-SHA1(secret, currenttime) → Grab offset from LSB → Select 4-bytes from offset → Perform bitwise AND with 0x7FFFFFFF → Calculate mod 1,000,000 of resulting integer

HMAC-SHA1(LJICW6SQJMZ WQUZQ, 1328041514) → 99c8f6a1eab588d621 608d38bf88649a7e0 addd6 → 99c8f6a1eab588d621 608d38bf88649a7e0 addd6 → 0x88d62160 & 0x7fffffff = 0x08d62160 (148250976) → 148250976 % 1000000 = 250976

Source: https://devcentral.f5.com/articles/two-factor-authentication-with-google-authenticator-and-apm