

## Didi-server

### 1. Descripción:

Backend principal de la aplicación, permite almacenar los datos de recuperación de usuario y actúa como intermediario entre los demás módulos y mouro validando certificados y evitando que issuers no autorizados puedan emitir certificados.

### 2. Ejecución

#### a. Instalar Node:

Este módulo utiliza npm como gestor de paquetes, el cual viene integrado con Node: <https://nodejs.org/en/>

#### b. Instalar dependencias:

Abrir una terminal en la carpeta principal del módulo (a la altura del archivo 'package.json') y ejecutar el comando '**npm install**'

#### c. Ejecutar Didi-server:

A la misma altura, ejecutar el comando '**npm run start \$ENV\_VARS**', donde \$ENV\_VARS son las distintas variables de entorno del módulo.

#### d. Variables de entorno:

Nombre	Obligatorio	Descripción	notas	ej
DEBUGG_M ODE	No	<i>si está en true se muestran más cosas por consola</i>	-	<i>true</i>
MONGO_DI R	Si	<i>dirección en la que está corriendo mongo</i>	<i>La instancia de mongodb no necesariamente es la misma que para el didi-issuer!!</i>	<i>127.0.0.1</i>
MONGO_PO RT	Si	<i>puerto en que corre mongo</i>	-	<i>27017</i>
MONGO_US ERNAME	No	<i>usuario admin en mongo</i>	<i>se lo puede omitir si la base de datos no requiere autenticación (inseguro!)</i>	<i>didi_admin</i>
MONGO_PA SSWORD	No	<i>clave de usuario admin en mongo</i>	<i>se la puede omitir si la base de datos no requiere autenticación (inseguro!)</i>	<i>uIERvZXMlLCJpYXQiOjE1MTYyMzkwMjJ9</i>
MONGO_DB	Si	<i>nombre de la base de datos dentro de mongo</i>	-	<i>didi</i>
PORT	Si	<i>puerto en que corre didi-server</i>	-	<i>3000</i>

ADDRESS	Si	<i>dirección en que corre didi-server</i>	<i>Se la requiere para disclosure requests</i>	<i>http://192.168.2.113</i>
SERVER_D ID	Si	<i>did del didi-server</i>	-	<i>0xf1232f840f3ad7d23fcdaa84d6c66dac24efb198</i>
SERVER_P RIVATE_K EY	Si	<i>clave privada del didi-server</i>	-	<i>d8b595680851765f38ea5405129244ba3cbad84467d190859f4c8b20c1ff6c75</i>
MOURO_UR L	Si	<i>dirección en la que esta corriendo muro</i>	-	<i>http://192.168.2.113:3001/graphql</i>
MAILGUN_ API_KEY	Si	<i>api-key de la cuenta de mailgun</i>	<a href="https://app.mailgun.com/app/sending/domains/">https://app.mailgun.com/app/sending/domains/</a>	<i>6c8cb3c593fa1cf61d08846ed5111373-816b23ef-84fed409</i>
MAILGUN_ DOMAIN	Si	<i>identificador de la cuenta de mailgun</i>	<a href="https://app.mailgun.com/app/sending/domains/">https://app.mailgun.com/app/sending/domains/</a>	<i>sandbox07243b2823a94906b1c5e430f1caabdb.mailgun.org</i>
NO_EMAIL S	No	<i>si esta en true no envia los mails</i>	<i>Si no está definido, el mail se envia</i>	<i>true</i>
TWILIO_S ID	Si	<i>identificador de la cuenta de twilio</i>	<a href="https://www.twilio.com/console">https://www.twilio.com/console</a>	<i>AC586bd7b08e0fc1e687a7913cf6eddc86</i>
TWILIO_T OKEN	Si	<i>token de la cuenta de twilio</i>	<i>a33201fbebba1232017e5ff0d3fc12cf</i>	<i>a33201fbebba1232017e5ff0d3fc12cf</i>
TWILIO_P HONE_NUM BER	Si	<i>número desde el que se envían los sms</i>	<a href="https://www.twilio.com/console/sms/getting-started/build">https://www.twilio.com/console/sms/getting-started/build</a>	<i>+12568264160</i>
NO_SMS	No	<i>si está en true no envía los sms</i>	<i>Si no está definido, el sms se envia</i>	<i>true</i>
SERVER_I P	Si	<i>ip del didi-server</i>	<i>requerido por renaper</i>	<i>192.168.2.113</i>
RENAPER_ SCORE_TR ESHOULD	Si	<i>minimo grado de certeza para aprobar un mach del renaper</i>	-	<i>75</i>
RENAPER_ API_KEY	Si	<i>api key de renaper</i>	-	<i>50f32205-ee2e-4045-8614-47a8f74280c2</i>
RENAPER_ API	Si	<i>api de renaper</i>	-	<i>https://renaperpreprod.dn.m.gob.ar/</i>
RENAPER_ URL	Si	<i>url de renaper</i>	-	<i>http://onboarding.renaper.prod.vusecurity.com:8080/vu-onboarding-rest/onboarding/</i>
RSK_URL	Si	<i>Url donde se encuentra corriendo</i>	-	<i>https://public-node.testnet.rsk.co:443</i>

		<i>La blockchain donde se almacena la información de delegación</i>		
BLOCKCHAIN_URL	Si	<i>Url donde se encuentra corriendo la blockchain</i>	-	<i>https://mainnet.infura.io/v3/21d2ee9de6484541b66eb06942ceb3c7</i>
BLOCKCHAIN_CONTRACT	Si	<i>Identificador del contrato de ethr-did-registry dentro de la blockchain</i>	-	<i>0xdca7ef03e98e0dc2b855be647c39abe984fcf21b</i>
BLOCKCHAIN_DELEGATION_DURATION	no	<i>Tiempo en segundos durante el cual una delegación de did es válida.</i>	-	<i>Default 1300000 (1año)</i>
HASH_SALT	Si	<i>Salt a ser usado al encriptar datos indexables (mail, tel)</i>	-	<i>\$2b\$11\$ggDdDiXNBkuEiQWTdHQ.hu</i>
FIREBASE_URL	Si	<i>Url de firebase (requerida para push notifications)</i>	-	<i>"https://didi-6fd49.firebaseio.com"</i>
RSA_PRIVATE_KEY	Si	<i>Clave privada a utilizarse al encriptar los datos con rsa</i>	-	<i>Ver abajo...</i>
FINGERPRINT_DATA	Si	<i>fingerprint del dispositivo donde se corre didi-server</i>	<i>generado con el "Browserfingerprint.rar" que me paso Eze</i>	<i>Ver abajo...</i>

RSA\_PRIVATE\_KEY:

-----BEGIN RSA PRIVATE KEY-----

```

MIIBOwIBAAJBAAO64JHU8uFH4ZsmhbkGUFysU/GktjV3vT84TfGjKljw6npCbFMeN
QZmmSa+TQb+oYurIO2YOaw5GI4LfQbkjnpCawEAAQJACEWrRcC/5I9EOJJ2fqFC
GEUW5hIIBu9HBa4ZLoxqmUmhmPhov5if2ga1IE9vpcTOzmGIMW/LPBGS184wW6tG
IQIhAPfwR5vkrSYkDudw6Sp5uwsTv1t2sMT3bWwhDJDquv1RAiEA9nsgNrc1Y95c
+YVHr6e4v4bZYcxsHV5WE8ZCC5EDw2cCIQCmPZ9I8W//UNIFcHmGF1TIWpdFIIFz
34qoo4gvapOx4QIhAIdVc4qXbak4HrSiiYnY/Yer8w/Pvk0hzwFsijbvmLFhAiBB
JoZfex8gJUKiNfKXYtJkBFy2fTOQ7c1iEDS6hnlKSA==

```

-----END RSA PRIVATE KEY-----

## FINGER\_PRINT\_DATA:

[illegible]

QifSwib3MiOnsibmFtZSI6Ik1hYyBPUylsInZlcnNpb24iOilxMC4xNC42In0slmRldmljZSI6e30slm  
NwdSI6e319fQ==”