June 18, 2019

Whitepaper
Dynsecu, a decentralised application

(by Ivan Peeters, inventor)

1. Introduction

DYNSECU is a technology platform based on cognitive authentication technology that uses the unique profile of each individual.

This new and unique technology can provide a log-in service in which the user never has to remember his log-in codes and because the cognitive authentication codes are a part of the mind of the user, it's nearly impossible to be hacked.

The technology can be used for IoT platforms, the security of (mobile) apps, crypto wallets etc.

2. How does it work?

The user has to "program" his own profile only a first time and then can log-in by simply answering a couple simple questions (also called "challenges"). These answers are unique for every person and can only be answered by the user and not by anyone else.

In contrast to other (so called "static") log-in technologies, the user does not have to remember passwords and/or pin codes, or does not need special hardware and/or biometrics. At any time the user want to log-in he or she only has to recognize his or her "valid" answer among other "false" answers.

Because the user does not has to remember anything , he or she can never forget the password and in addition, it's impossible for a third person to recognize the "valid" answers.

3. Why is this technology unique?

With this kind of technology the user can't forget his answers, but on top of this it's also a so called rolling code. Every time the user logs in, he or she gets different "rolling" of so called "dynamic" questions (challenges) in a different combination between different dummies. This makes it nearly impossible to hack the login.

But we take it also a step further. We developed a M2M (machine to Machine) application based on this technology what results in a rolling code between machines "programmed" by the user.

This technology has several patents (granted and pending) and there are already ongoing negotiations with tech companies.

4. Significant contribution

Is suitable for many different applications:

IoT platforms: M2M rolling codes in combination with personal (cognitive) codes

- Crypto wallets
- Wireless car keys
- Online bank apps
- etc.

Because of the flexibility of the technology the integrations are limitless. It can be integrated be also used as add on to already existing applications.

5. Usability

Is suitable for many different applications:

- IoT platforms: M2M rolling codes in combination with personal (cognitive) codes
- Crypto wallets
- Wireless car keys
- Online bank apps
- etc.

Test:

We have tested this application with the help of 16 test persons:

- ✓ 3 test persons > 60years
- ✓ 2 test persons > 40years<60years
- ✓ 5 test persons > 30years<40years
- ✓ 4 test persons > 20years<30years
- ✓ 2 test persons < 20years

The conclusion:

Only for the group > 60 years the set up was a little difficult but the lack of knowledge of the English language was also an extra factor.

For the other test persons the registration and log in procedure was no problem. The reaction on the login procedure was overall very positive.

6. Reliability

- The use of a “mini blockchain” in the backend guarantees operation
- The user can make several mistakes
- If the user loses his mobile device there is a backup procedure
- A backup of the wallet of the mobile phone can be stored in the “mini-blockchain”

7. Security

- Only the user knows all the passwords
- The backup provider(s) “knows” only a part of the solution
- The hacker has to know all the users passwords and has to have the mobile device in his hands
- The communication between different devices are always M2M and never an user interface in combination with a network

If the network noticed a possible attack of a hacker the account can be blocked and the user can deblock his account himself.

Operational availability measurement are not performed because of the limitations of the demo version. We only provide a technology that can be implemented. The performance of the system itself is a result of the technology used by the provider.

8. Privacy and data protection

- All data and security passwords are stored fragmented and spread over the different servers in the mini-blockchain.
- The personal information can be stored in a secure environment on the providers server in combination with the “mini-blockchain”
- The “mini-blockchain” is not an open ledger but a combination of different servers working like a blockchain but is closed for the outside and monitored by different entities

9. Applicability

The technology can be used in the following sectors:

- Health: communication with doctors can be secured using different levels of security. Above that the mini-blockchain can register who has consulted which kind of information.
- Transport: the M2M communication connects different devices with a rolling code that is unique for each user.
- Finance: the wallet can have different security levels.
- Telecom: connecting the mobile phone to an unique user login makes it also possible to block the mobile device if this get stolen
- Governmental: the security can be used online but also offline (e.g. counter)
- Energy: connected to a secured IoT platform the smart meters, switches and valves can also be secured

10. Compatibility

- Can work with any kind of OS system
- Compatible with any kind of wireless software: Wi-Fi, Bluetooth etc.

11. Affordability

- Because the use of a mini-blockchain the cost of use is minimal,
- The information per server is only a part of the info
- Only a limited number of servers are been used
- On users side almost any smartphone can install an app with Dynsecu technology. The Dynsecu technology will increase the app with max 1MB
- Estimated costs

We believe that the future of our technology will be meanly in the field of IoT. Simply because this is the next big thing and our technology could be a perfect match in this field.

There are many possible applications in different fields, to illustrate our technology in a understandable application we made a virtual financial wallet (coins).

12. Demo

One of the applications that has a huge benefit using our cognitive authentication technology are the so called cryptocurrency wallets.

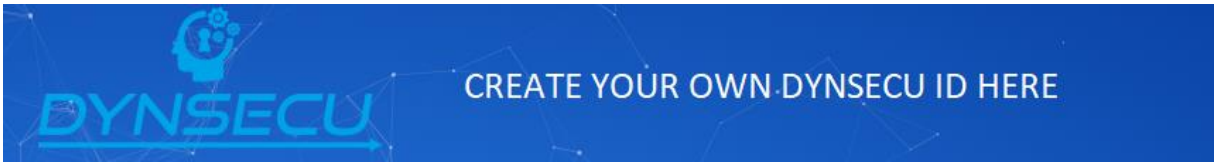
The security of these wallets are the biggest problem at the moment, especially when it comes to the online versions, who are the most practical ones.

In this paper we shows how to use our technology in a crypto coin application using the DYNSECU technology to secure the cryptocurrency wallet.

Before the wallet is active the user has to “program” his own profile only a first time and then can log in by simply answering a couple simple questions (also called “challenges”).

Dynsecu is not only an idea protected with a patent pending procedure but has also a working demo that can be found on the website: http://www.dynsecu.com/

Link to the working demo:



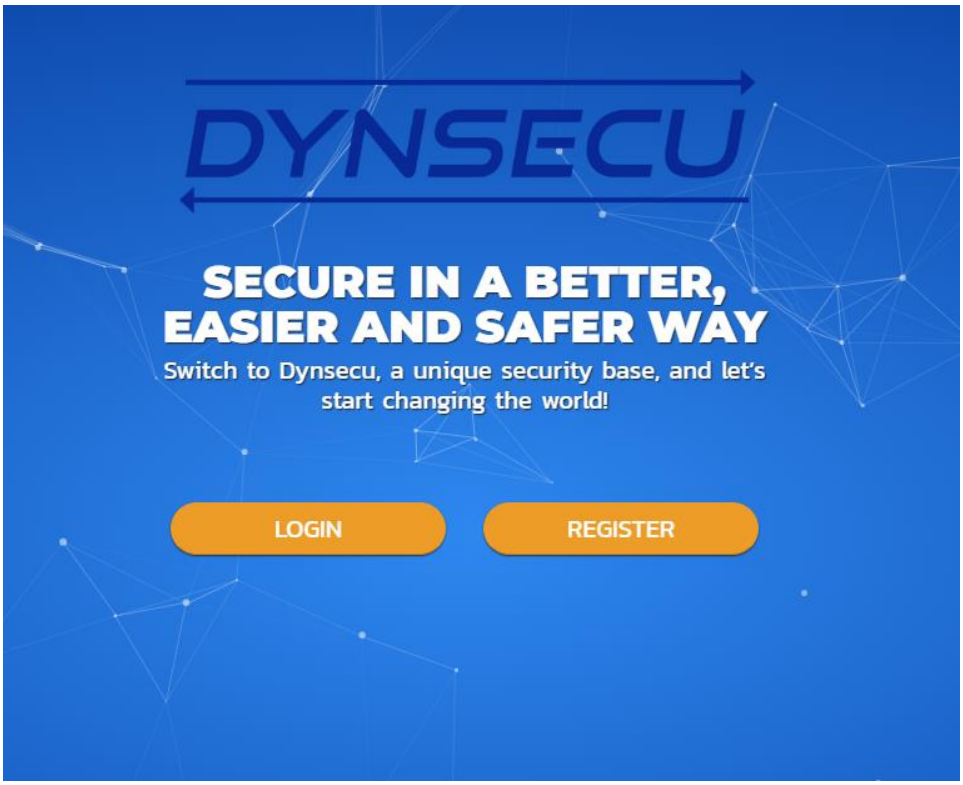
(The link is: https://dynsecu.io/ the URL can be changed, therefore the advice is to use always the link on the website)

If username and password is asked, please fill in codes below)

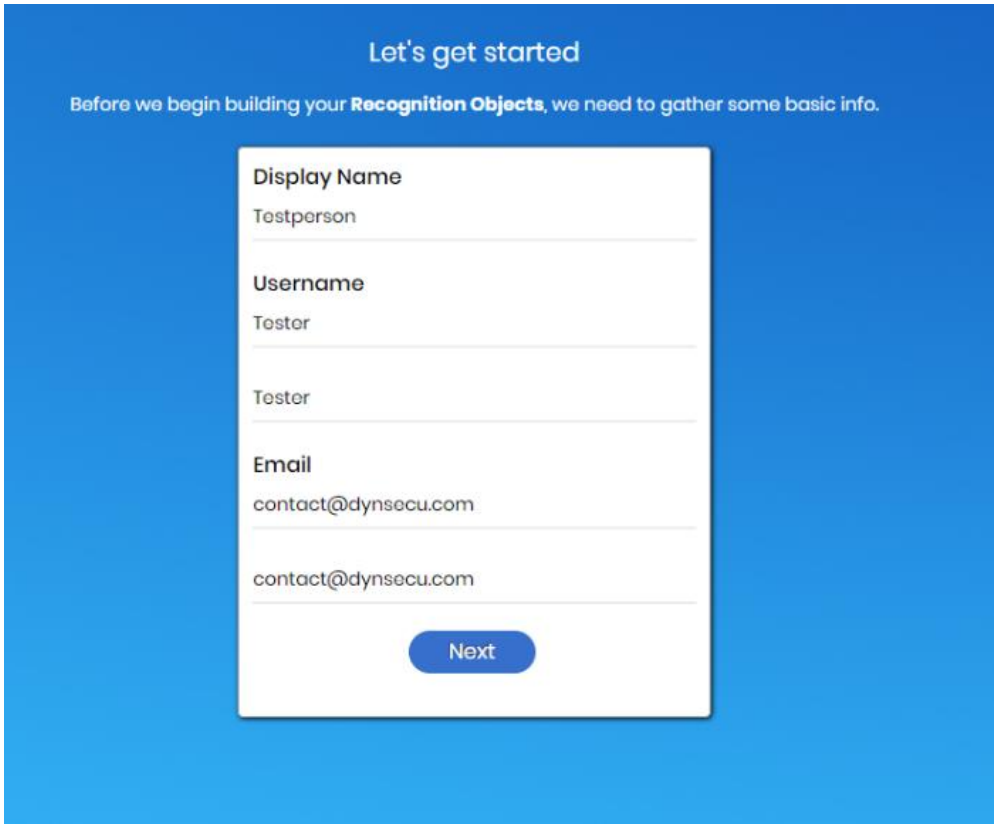
(Username: demo - password: dynsecu2018)

Use of the demo:

First time use: registration



First the id of the registrant

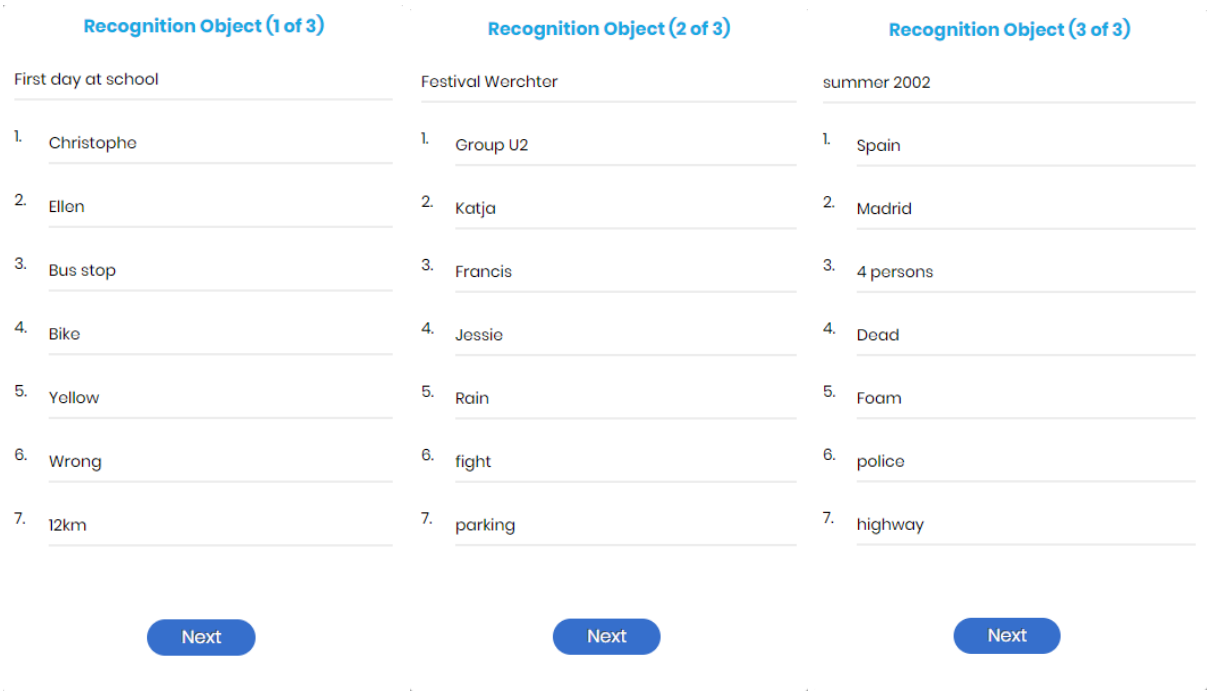


Time to create your own recognition objects

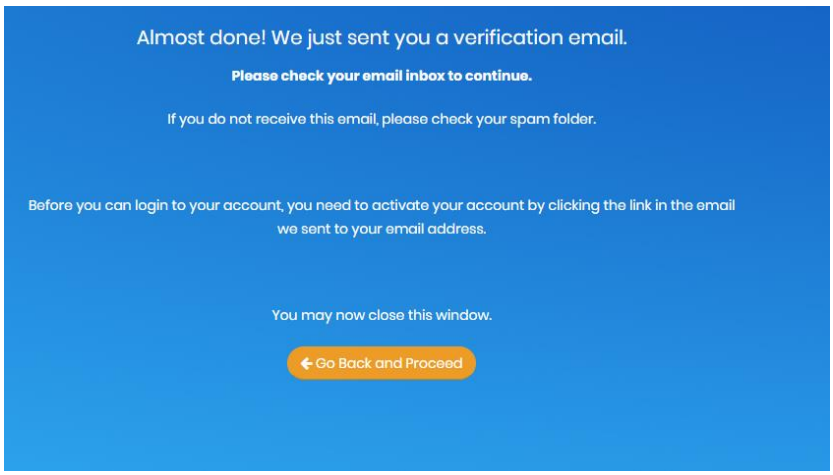
Remember a recognition object is a focus object coupled with attributes that have special meaning to you.

You may now begin by filling in the blanks below to create your own Recognition Objects.

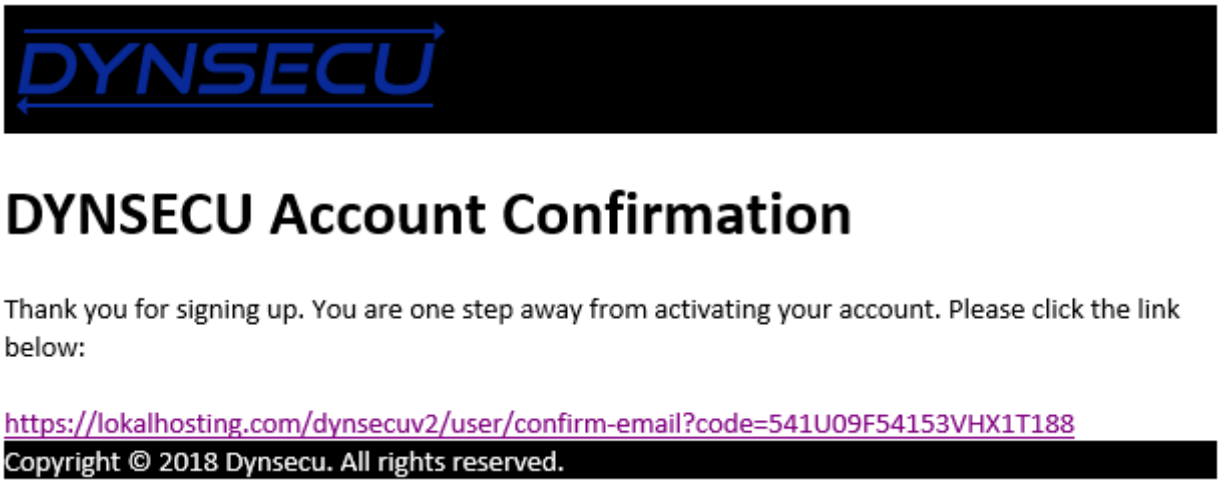
Create your Recognition Objects and Attributes using English words, except of course for dates of years, proper names, names of cities and places. Other language versions of Dynsecu will be released later.



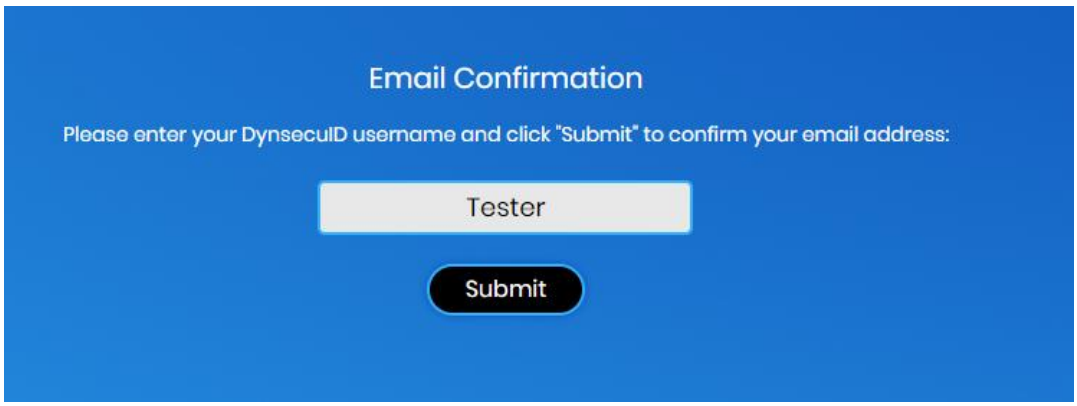
Time to check your email!



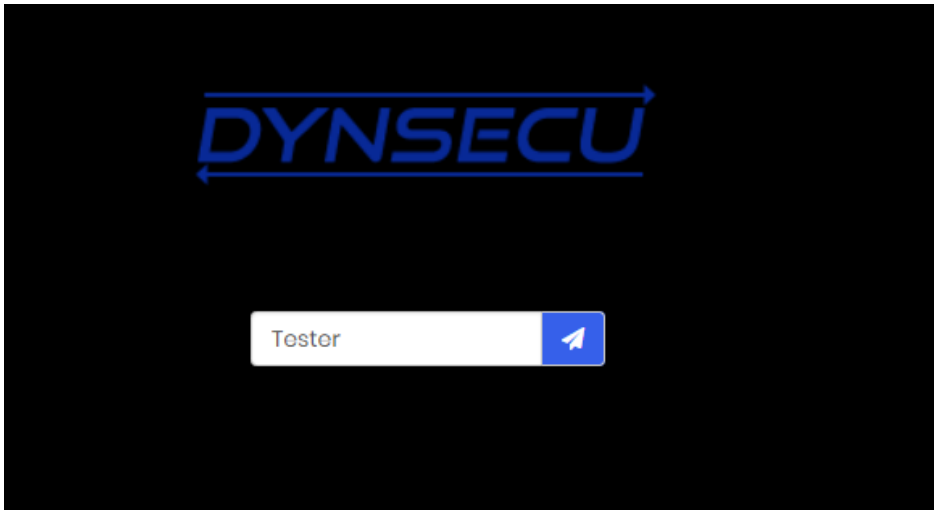
Click on the link in the mail



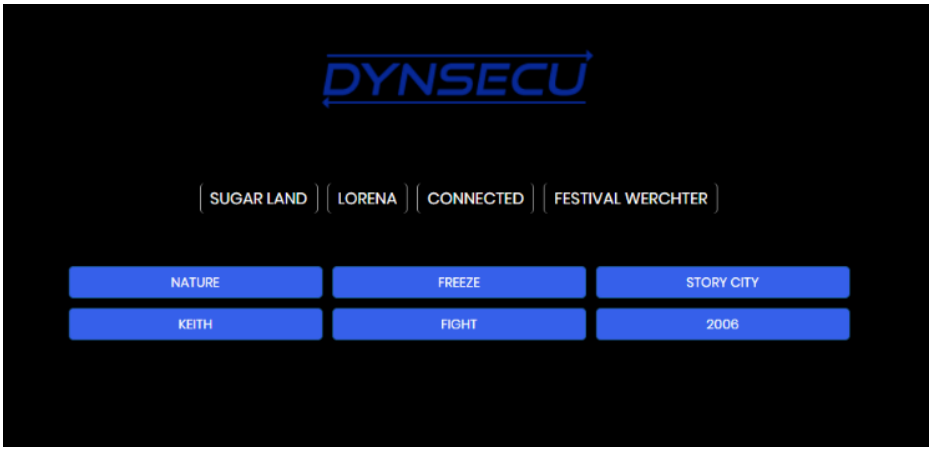
Confirmation of the mail:

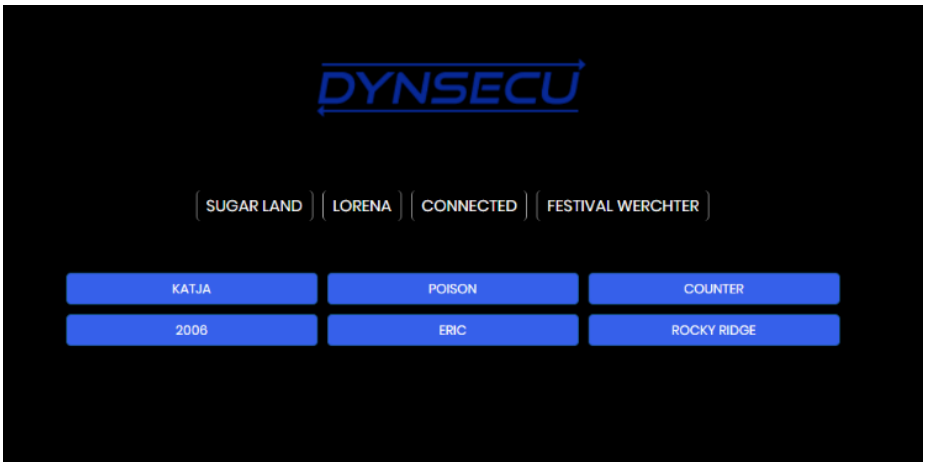


Start the login procedure:



Answering 5 questions





Personal identification

Dynsecu will now ask you to identify yourself. This is to ensure the **"one-user-one-ID"** policy, and other policies and regulations such as preventing illegal or criminal usage of **Dynsecu**. Once your profile is approved, **Dynsecu** will dis-connect your profile from your **personal ID data**, so under no circumstance any third party (for example an intruder - can ever trace you. Your personal ID data will be kept off-line, only for usage by Dynsecu staff in case contact with you, the user, needs to be established and such contact cannot be established via your **cognitive ID**.

Firstname: Tester
Lastname: person
Country of Birth: België
Date of Birth: 01/01/1980

Please attach a scan or picture of a valid ID card, driver license, passport, etc. containing your photo

Bestand kiezen | Geen bestand gekozen

Submit

13. What are the problems with the current applications?

A. Wallets (prognose to the near future)

There are 4 kind of wallets

- The online wallet
- The software wallet (app)
- The hardware wallet (usb stick)
- The paper wallet

The first 2 are the most user friendly but relatively easy to hack. The paper version is almost impossible to use and can't be protected with a password. The conclusion is that the hardware wallet the best is of the 4.

But the hardware wallet has also disadvantages

In case of a USB stick, it can't be used in combination with a tablet or smartphone - It can be stolen - You have to carry it always with you if you want to use it - It's a step back in the modern development.

B. App's
All financial providers using app's to make provider their clients additional services. However the present technologies such as fingerprint or facial recognition are still not sufficient enough. If a hacker using the so called Trojan horses he can still get the codes.

C. Problems with biometric and 2-way authentication
One of the biggest problems with biometric and 2- way authentication is that once these data has been hacked and they are in the hands of third parties, these data is been compromised and can never been used again. This is not the case with our technology.

D. General log-in procedure
Current log-in procedures often require remembering different passwords, replying to e-mail addresses, and systematically changing passwords to prevent hacking in a certain time frame.

Dynsecu is patent pending technology!

www.dynsecu.com