augmented security

Solution Universelle d'Authentification Forte

What are we taking about ?

Cybercrime costs the global economy $1,000 billion a year, half as much as two years ago!

Between ransomware and hacking, cybercrime is looking to diversify

There are legal obligations

DSP 2

Payment Services Directive 2

Stricter security standards for online payments to increase consumer confidence in online shopping.

Strong authentication

Strong authentication, or two-factor authentication, combines the use of two elements from three categories: something you know (password, pin code), something you have (computer, cell phone), something you are (fingerprint, retina, voice).

What is our strong point

In a world where our data (professional and personal) is worth its weight in gold

- Access by simple "Login/Password" is illegal for any purchase
- Increase in hacking
- Development of e-commerce
- Too many different passwords slow down operations and create purchase abandonment
- SMS is easily hackable

Augmented Security has been awarded a European patent
Demonstrating it is a strong, unique and simple solution.

Enrollment phase 1

PRELIMINARY

- Download the IOS or Android application
- Fill in the personal data
- Works on any smartphone … any IOT or PC's

01

Enter your login information

02

Enter the activation key

Enrollment phase 2

03

Enter your secret code

04

Ready to use

Authentication connected mode

01

IDENTIFY

by the possession of its device

02

SELF-IDENTITY

by its secret code

03

AUTHENTICATION SUCCESSFUL

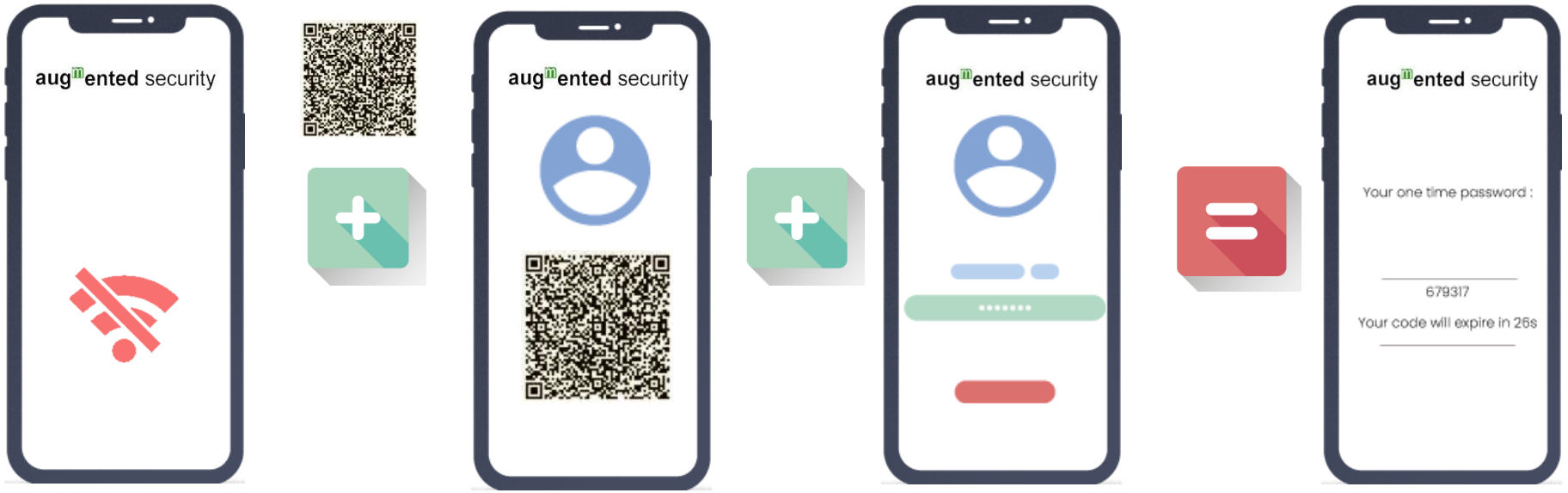
Authentication disconnected mode

01
Application launch

02
Scanning the QR Code

03
Entering the pin code

04
OTP Generated



High security" user benefits

User identity protection

- User data stored in encrypted format on the authentication server
  authentication server (cryptographic processing)

Secure smartphone application

- No data stored by the smartphone application
- Fully "offended" code (hidden system calls...)

Ease of use

- Instinctive customer journey
  Validation by a simple PIN code chosen by the customer.
- No information stored on the smartphone.
- If the phone is lost/stolen, even if it is unlocked
  the application is unusable
- SIM card and terminal independent solution

High security features

Patented strong 2-factor authentication

- Hardware signature of the smartphone (processor serial number...) or equivalent
- **Personal code defined by the user during enrolment. Always the same**

3 levels of resistance to "Man In the Middle" attacks

- Smartphone - Authentication Server link realized in HTTPS/TLS V1.2
- Encryption of all exchanged data by AES session key
- Over-encryption of sensitive data (SHA2, Bcrypt)

Resistance to Phishing

- AES session key sent by the smartphone application encrypted by the public key of the authentication server
- Server authentication certificate verified by the smartphone application
- Unique public/private key for each authentication server
- SAML protocol support for Single Sign On (SSO) authentication

In a nutshell

01 **Simplification of PSD2:** User password used, not the one sent by the provider.

02 **Personal code** defined by the user during enrolment.

03 **European patent**, French know-how

Automotive market & more

Public bodies

e-university

e-administration

e-health

e-vote

Companies

Network/web access

Physical access

Cybersecurity

Retail

Transportation

Social networks

Banks

Home banking

Cash withdrawal

Money transfer

M-payment

e-commerce

augmented security

Solution Universelle d'Authentification Forte

Jacques PAUCKER
President
jacques.paucker@augmented-security.net
+33 (0)6 86 13 10 26

Charles ORSEL des SAGETS
Partner, in charge of business development
charles.orseldessagets@augmented-security.net
+33 (0)6 72 86 71 90

Press release embargo 01.02.2022

Jacques Paucker takes over **Augmented Security** and announces that their strong authentication solution simplifies the validation process while meeting the **DSP2** standard.

Their patent makes it possible to secure and protect connected vehicles from criminal penetration, while avoiding the need to receive a new code at each checkout.
Automotive specialist Jacques Paucker was president of Logikko, a company he co-founded in 2013, until March 2021.

This company, in which he remains a shareholder, is a committed player in the ecological transition by developing a patented technology based on hydrogen injection to improve combustion in combustion engines and drastically reduce their pollution.

Today, another fundamental field is open to breakthrough innovations: M2M security between an engine and the Internet. Indeed, these transactions are not secured, which allows, for example, to take total or partial control of a car, bus, truck or boat engine....

Today, **Augmented Security** is a true disruptive technology based on the material signature of a vehicle owner's communication component.
Jacques **Paucker** explains: "*In the world of the connected vehicle, serious cyber security issues arise. Augmented Security provides the assurance of a superior level of security for all access to vehicle and user data.* "