Development of a software module based on a patented protocol to drastically reduce fraud in applications exchanging encrypted and authenticated information end-to-end

Summary

Profile type	Company's country	POD reference
Technology offer	**Spain**	**TOES20250217007**
Profile status	**Type of partnership**	**Targeted countries**
PUBLISHED	**Investment agreement** **Commercial agreement with technical assistance** **Research and development cooperation agreement**	• **World**
Contact Person	**Term of validity**	**Last update**
Enrico FRANZIN	**17 Feb 2025** **17 Feb 2026**	**17 Feb 2025**

General Information

Short summary

A group of researchers in communications security from a leading University in Madrid (Spain) aim to develop and commercialise a software module and associated interface that implements their already patented secure communications protocol, suitable for its application in IoT platforms, online banking authenticators (2FA authenticators) or messaging. They are looking for partners with experience in the development and integration of secure software products into applications.

Full description

It is common in the Internet that the security of communications is mainly based on the use of https, which:
- does not encrypt the information directly in the communicating Apps, leaving areas where the information can be captured in readable form.
- does not perform a mutual authentication of the communicating parties, which leaves an open door to phishing attacks.
- makes use of a Digital Certificate, sometimes issued by a third party entity that is not "trusted".

According to experts, all these vulnerabilities are at the origin of 80% of cybercrime, which is estimated to increase from 9.22 in 2024 to 13.82 trillion dollars in 2028.

These weaknesses of https need to be covered by applying a new protocol to the communicating applications themselves that: performs end-to-end encryption to avoid areas where information travels over the Internet in a readable form; requires mutual identification of the communicating applications to avoid impersonation; avoids the intervention of third parties, not always trusted, in the identification of users.

These are some of the contributions of the innovative patented communication protocol that with this project will be implemented in two pieces of software that will later be incorporated into the communicating applications to make their communications secure and avoid fraud.

Its implementation in the applications achieves that the security of communications is independent of the medium that communicates them and, therefore, it is not incompatible with continuing to use https, or any other protocol, that is already being used.

Some case uses: Authentications and secure online operations in banking, e-commerce, online payments; creation of secure communications channels with interest in e-administration, health, law enforcement; Internet of Things; etc.

The group of researchers is looking for partners with experience in the development of secure software and its integration in applications, as well as with experience in the commercialization of software products and software maintenance.

Advantages and innovations

The protocol to be implemented makes important contributions to the state of the art in communications security: Its communications meet all the requirements demanded of secure communication: confidentiality, integrity, mutual authentication and non-repudiation; Communications are kept secure end-to-end; The protocol adds a new layer of security on top of the network protocol itself that communicates the applications.
Economic benefits:
1. Assuming the experts' predictions are accurate, namely (a) the global cost of cybercrime will increase from $9.22 trillion in 2024 to $13.82 trillion in 2028, and (b) impersonation and exploitation of vulnerabilities for information capture are the source of approximately 80% of attacks, implementation of the new protocol could save more than $36 billion over 4 years, from 2024 to 2028.
2. Its incorporation into online payment systems allows these systems to be adapted to the European online payment regulations known as PSD2.

Technical specification or expertise sought

The partner must have experience in: communications security software; secure network software; development of secure software and its integration in applications; marketing of software products; participation in international subsidized projects; software maintenance.

Once the project that develops the pieces of software that support a network with secure communications has been executed, it is desirable that the same collaborating company has the capacity to market, implement and maintain the protocol software in the communications networks that use it.

Ideal partners will be located in the European Union, the United States and Mexico, since these are the countries in which the protocol's patent is registered and, therefore, they have exclusive rights to its commercial exploitation.

Stage of development

Concept stage

Sustainable Development goals

- **Goal 9: Industry, Innovation and Infrastructure**

IPR Status

IPR granted

IPR Notes

Partner Sought

Expected role of the partner

Partner shall:

- Elaborate and agree, with the Research Center and the owners and inventors of the protocol patent, the software development plan that will allow the creation of application platforms characterized by the exchange of secure communications that apply the patented communications protocol.

- Elaborate and agree, with the Research Center and the owners and inventors of the protocol patent, the commercialization plan for the developed software.

- Agree, with the owners of the protocol patent, the license to use the patent and the software to be developed.

- Execution of the development plan for the piece of software that:
1 - Allows incorporation of the patented communication protocol in the communicating applications so that it is executed when the applications exchange information over vulnerable networks;
2 - Manages the applications that are part of the application platform with secure communications, and the secure distribution of the keys shared by each pair of communicating applications.

- Execution of the marketing, integration and maintenance plan for the developed software.

Type of partnership

Investment agreement

Commercial agreement with technical assistance

Research and development cooperation agreement

Type and size of the partner

- **SME 50 - 249**
- **Other**
- **R&D Institution**
- **Big company**

Dissemination

Technology keywords

- **01003008 - Data Processing / Data Interchange, Middleware**
- **01006005 - Network Technology, Network Security**
- **01006013 - Communications Protocols, Interoperability**

Market keywords

- **01006001 - Defence communications**
- **02007013 - Banks/financial institutions software**
- **02007007 - Applications software**

Targeted countries

- **World**

Sector groups involved

- **Digital**
- **Aerospace and Defence**