Secure Societies 2024: Horizon Europe Cluster 3 Brokerage Event in Istanbul Pitch Presentation Template

Alicia Jiménez
GRADIANT

REPUBLIC OF TÜRKİYE
MINISTRY OF INDUSTRY
AND TECHNOLOGY

#NATIONAL TECHNOLOGY INITIATIVE

enterprise europe network
Business Support on Your Doorstep

Sabancı Üniversitesi

İSO

TÜBİTAK

QBeCAS: Quantum Beyond Cryptographic Algorithms and Standarization

Contact Details

- Name: Alicia Jiménez González
- Organization: Galician Research Center in Advanced Telecommunications
- E-mail: ajimenez@gradiant.org
- Telephone: +34 669886952
- Country: Spain

Proposal activity: HORIZON-CL3-2024-CS-01-02

Description of the Organization

- *Expertise of your company/ previous Projects*
- ICT technologies focused on three main topics:
  - Communications
  - Security
  - Intelligence

  Gradiant has taken part in more than 35 European projects, including communications for unmanned vehicle s, payloads integration, data analytics and security measures.
- *Expertise related to the topic*

- Projects
  - Facendo 4.0: development os a system to automatically push updates (included cryptographic keys) to IoT devices in a centralized way. The updates are signed by a key protected by a HSM.
  - xAIAL: Development of module to create a cryptographic inventory of the cryptographic keys and digitals certificates of the devices of an organization with capabilities to renew this material whenever is needed from a centralized node.
  - CICERO: Research and development of a prototype to automatically detect cryptographic algorithms used by a system.
- Expertise on hardware platforms
  - HSMs: general purpose, financial, programmable
  - TEEs: Intel SGX and TDX, AMD-SEV

Alicia Jiménez/ ajimenez@gradiant.org

Proposal idea/content

- *Role in the project : partner (possible coordinator)*

- Objectives:
  - to ease the transition from the pre-quantum era to the post-quantum one
  - to provide recommendations on how to implement post-quantum algorithms to increase their widespread
  - to contribute to standardization and regulatory activities for post-quantum cryptography

- Expected results
  - to contribute to the standardization of currently proposed post-quantum algorithms
  - to develop a tool that allows to automatically identify and assess the security of cryptographic material used by applications
  - to develop a set of tools that ease the transition of applications to post-quantum cryptography
  - to validate the research and implementations across several use case pilots

Alicia Jiménez/ ajimenez@gradiant.org

Proposal idea/content

- *Description of the proposed project idea*
  - *QBeCAS will take a crypto-agile approach developing tools with the aim of identifying cryptographic material (both keys and software) to* ***identify vulnerabilities*** *and start the transition to post-quantum algorithms*
  - *QBeCAS will target both existing and new applications, giving* ***recommendations*** *on how to update the cryptographic algorithms.*
  - *QBeCAS will also explore post-quantum algorithms* ***standards*** *by international standardization entities (like NIST) to assess their maturity and applicability proposing hardware implementations to accelerate them (****HSMs****) and to secure them in untrusted environments (****TEEs****).*
  - ***Several use cases*** *will be considered like Public-Key Infrastructures and core applications of financial institutions that heavily rely on the security of cryptograpy.*

Project participants

Existing Consortium - profile of known partners (if any)

No	Partner Name	Type	Country	Role in the Project
01	GRADIANT	RTO	Spain	Research and implementation in crypto-agility, tools and PQC
02	University of Napoles	UNI	Italy	In discussions
03	Kleuven	UNI	Belgium	In discussions
04	Thales	LE	France	In discussions
05				
06				
07				

Project participants

Consortium – required partners

No	Expertise	Type	Country	Role in the project
01	PKI – Public key Infrastructure			Use case
02	Standarization			Partner, contribution to standarization activities
03	Post quantum cryptography	Uni		Research and implementation of PQC
04	Financial	Bank		Use case
05				
06				