

PLIEGO DE PRESCRIPCIONES TÉCNICAS DEL PROCEDIMIENTO ABIERTO DE ADJUDICACIÓN DE UN CONTRATO DE SERVICIOS PARA LA REALIZACIÓN DE ALGORITMOS SOFTWARE DE CIFRADO HOMOMÓRFICO Y CIFRADO LIGERO PARA SU UTILIZACIÓN EN ENTORNOS INDUSTRIALES

1.- OBJETO

Los servicios objeto de este contrato son la Investigación, Diseño, Desarrollo, Implantación y Mantenimiento final de algoritmos de cifrado homomórfico y de cifrado ligero en sistemas industriales.

Entendemos por criptografía homomórfica EL conjunto de técnicas criptográficas que permiten operar con datos cifrados de tal forma que, al descifrarlos, los resultados de las operaciones se manifiesten sobre el dato en claro.

Los Algoritmos de Criptografía Homomórfica a investigar, desarrollar y probar son:

- Partially Homomorphic Encryption
- Somewhat Homomorphic Encryption
- Sistemas basados en control de ruido
- Sistemas de aproximación y truncado
- Fully homomorphic encryption

Entendemos por criptografía ligera (i.e., LwC por sus siglas en inglés) al conjunto de procedimientos criptográficos centrados en proporcionar soluciones que garanticen la confidencialidad e integridad de la información en dispositivos limitados en computación y energía, sin perder el rendimiento pedido a la tarea o tareas principales del sistema. Los Algoritmos de Criptografía Ligera a investigar, desarrollar y probar son:

- ASCON
- COMET
- DryGASCON
- Elephant
- PRESENT
- CLEFIA
- SIMON y SPECK

2.- PLAZO DE EJECUCIÓN

El plazo de entrega del software y de la realización de las pruebas unitarias, de integración y de rendimiento en un entorno industrial será de 3 meses desde la firma del contrato.

Código Seguro De Verificación	cUh4YQ7oEHUf8cFVGWlZzg==	Estado	Fecha y hora
Firmado Por	María Teresa del Val Núñez - FGUA	Firmado	21/08/2022 23:54:01
Observaciones		Página	1/2
Url De Verificación	https://vfirma.uah.es/vfirma/code/cUh4YQ7oEHUf8cFVGWlZzg==		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		



3.- IMPORTE MÁXIMO DE LICITACIÓN

El importe máximo de licitación para el presente contrato se establece en 70.180 € IVA incluido. Este contrato se configura como de tracto puntual, y no podrá ser adjudicado por un importe superior al presupuesto de licitación, abonándose el precio de adjudicación únicamente en un pago.

4.- OTRAS CONDICIONES DE EJECUCIÓN DEL CONTRATO

La empresa adjudicataria está obligada a proporcionar el software que implementa los algoritmos reflejados en el punto 1 OBJETO (5 de Criptografía Homomórfica y 7 de Criptografía Ligera) así como la documentación de las pruebas realizadas que demuestran su funcionamiento.

5.- LUGAR DE ENTREGA Y PRUEBA DEL SOFTWARE

La entrega del software y las pruebas se realizarán en los laboratorios de la Escuela Politécnica Superior de la Universidad de Alcalá en el Campus Científico - Ctra. Madrid – Barcelona Km. 32. 28805 Alcalá de Henares.

6.- PLAZO DE GARANTÍA.

El plazo mínimo de garantía para mantenimiento correctivo y evolutivo del software será de 1 año a partir de la realización de las pruebas y aceptación del software por parte de la FGUA-UAH.

7.- FACTURACIÓN

El suministro objeto del contrato generará su correspondiente factura. La factura se enviará al Departamento de Contabilidad. El plazo máximo de pago de la misma será de 30 días a contar su recepción, mediante transferencia bancaria a la cuenta indicada por la empresa adjudicataria.

8.- PROCEDIMIENTO Y FORMA DE ADJUDICACIÓN

- Procedimiento: abierto abreviado simplificado
- Forma: múltiples criterios

Código Seguro De Verificación	cUh4YQ7oEHUf8cFVGWlZzg==	Estado	Fecha y hora	
Firmado Por	María Teresa del Val Núñez - FGUA	Firmado	21/08/2022 23:54:01	
Observaciones		Página	2/2	
Url De Verificación	https://vfirma.uah.es/vfirma/code/cUh4YQ7oEHUf8cFVGWlZzg==			
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).			