MEMORIA JUSTIFICATIVA DE LA ADJUDICACIÓN DE UN CONTRATO DE SERVICIOS PARA LA REALIZACIÓN DE ALGORITMOS SOFTWARE DE CIFRADO HOMOMORFICO Y CIFRADO LIGERO PARA SU UTILIZACION EN ENTORNOS INDUSTRIALES

1.- NECESIDADES A SATISFACER MEDIANTE EL CONTRATO

Para realizar las labores de investigación, desarrollo de software y pruebas de validación encomendados en el Proyecto CIEN Cibersec es necesario contar con los medios humanos y materiales necesarios para ello, así como con el conocimiento y experiencia en ciertas técnicas criptográficas.

La llegada5G y el Industrial Internet of Things (IIoT) requieren de conectividad constante entre los sistemas embebidos en entornos industriales. Aquí entra la necesidad de incluir seguridad a las comunicaciones y almacenamiento de datos, dichos sistemas se comunican entre ellos de manera continua y comparten información de todo tipo, incluida información sensible y/o personal; o simplemente es peligroso su acceso no autorizado.

Estos sistemas cuentan con recursos computacionales y energéticos limitados, de manera que no podemos utilizar algoritmos criptográficos habituales en los ordenadores de uso general, servidores, etc.; no contamos con dicha potencia para ejecutarlos de manera cíclica, ahí entra la criptografía ligera y la homomórfica para casos más sensibles pero con mayor capacidad de cómputo.

2.- INSUFICIENCIA DE MEDIOS Y EXPERIENCIA

El equipo de investigación no dispone de medios propios ni de conocimientos para la realización y pruebas de software de un nivel de sofisticación tan avanzado en técnicas de cifrado y criptografía como el requerido.

Dada la premura de tiempo se necesita la contratación de su realización, así como el soporte para la realización de pruebas de integración y de rendimiento en entornos industriales.

3.- OBJETO DEL CONTRATO

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

4.- DETERMINACIÓN DEL PRESUPUESTO BASE DE LICITACIÓN

El presupuesto base máximo de licitación de este contrato es de 70.180 euros (IVA incluido) y se ha determinado en función del precio unitario de los servicios a desarrollar.

Este contrato se configura como de tracto puntual. El importe de adjudicación no podrá exceder del presupuesto de licitación, abonándose el precio únicamente en un pago inicial.

5.- PRESUPUESTO BASE DE LICITACIÓN.

El presupuesto se ha calculado en base a los precios y horas estimadas de trabajo del mercado actual.

6.- APLICACIÓN ECONÓMICA COMPLETA

La tramitación será con cargo al presupuesto del centro de coste 80040289 Proyecto CYBERSEC.

7.- PLAZO DE EJECUCIÓN (O PLAZOS)

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.

8.- LUGAR DE REALIZACIÓN O ENTREGA

El suministro 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.

9.- PROCEDIMIENTO Y FORMA DE ADJUDICACIÓN

- Procedimiento: abierto abreviado simplificado
- Forma: múltiples criterios

10.- CRITERIOS DE VALORACIÓN

Las ofertas económicas se ajustarán al modelo que figura en el Anexo del Pliego de Cláusulas Administrativas

Criterios de valoración

La valoración se realizará sobre un máximo de 100 puntos repartidos, según se indica a continuación, entre los siguientes criterios valorables.

Se otorgará la puntuación máxima a la oferta con mejor precio, con más años de experiencia y con personal más cualificado tanto en los ámbitos detallados en el apartado 2 como en las publicaciones del apartado 3, valorándose el resto de las ofertas de manera proporcional. En caso de empate en la valoración global el criterio “2 Experiencia en entornos criptográficos y de cifrado” será el criterio para el desempate, si prevalece el empate el 2º criterio será el criterio “3 publicaciones”.

1. Precio: **20 puntos**

2. Experiencia en entornos criptográficos y de cifrado: **35 puntos**

La experiencia que se valorará será aquella circunscrita a la Investigación, Diseño, Desarrollo, Implantación y Mantenimiento de Software de Seguridad en los siguientes ámbitos:

- Sistemas de Cifrado Ligero y Cifrado Homomórfico. **Hasta 9,5 puntos**
- Sistemas de Detección de Intrusos (IDPS). **Hasta 1,5 puntos**

- Sistemas de Single Sign-On, cifrado y Protección Perimetral. **Hasta 2,5 puntos**
- Proyectos de Seguridad bajo tecnologías CryptoX. **Hasta 4 puntos**
- Sistemas con Tokens criptográficos y PKI para identidad. **Hasta 2,5 puntos**
- Sistemas Cripto-Biométricos. **Hasta 1,5 puntos**
- Estructuras Algebraicas aplicadas a la Codificación y Criptografía. **Hasta 9,5 puntos**
- Desarrollo de protocolos criptográficos mediante inteligencia analítica para la seguridad. **Hasta 4 puntos**

3. Publicaciones científicas de calidad contrastada y participación en congresos, jornadas y seminarios relacionados con la materia. Se valorarán con la máxima puntuación las publicaciones científicas presentes en cualquiera de los dos índices del Journal Citation Reports, tanto en el JIF (Journal Impact Factor) como en el JCI (Journal Citation Indicator) siempre en la edición SCI/SCIE (Science Citation Index/Expanded). Se valorará con mayor puntuación las publicaciones situadas en el primer cuartil (Q1), seguidas de las del segundo cuartil (Q2), las del tercer cuartil (Q3) y, por último, las del cuarto cuartil (Q4). Para las conferencias y congresos se tendrá en cuenta las incluidas en el listado del índice Computer Research and Education (CORE), valorando con mayor puntuación las de CORE "A", a continuación las CORE "B" y por último las CORE "C": **Hasta 30 puntos**

- Publicaciones Q1. **Hasta 8 puntos**
- Publicaciones Q2. **Hasta 7 puntos**
- Publicaciones Q3. **Hasta 5 puntos**
- Publicaciones Q4. **Hasta 3 puntos**
- Congresos CORE "A". **Hasta 3 puntos**
- Congresos CORE "B". **Hasta 2 puntos**
- Congresos CORE "C". **Hasta 2 puntos**

4. Otros criterios valorables de forma automática: **15 puntos**.

- Ampliación de garantía. 5 puntos por año. Con un máximo de 3 años (hasta 12 puntos)
- Reducción plazos de entrega. 1 punto por semana de reducción del plazo (hasta 3 puntos)

11.- CONTENIDOS DE LAS OFERTAS

En la oferta deberán especificarse los criterios de valoración. La oferta recogerá el precio sin IVA y con IVA del producto. En ningún caso el precio podrá ser superior al importe de licitación.

El precio incluye todos los gastos que sean necesarios para asegurar el normal cumplimiento del suministro, como son los gastos generales, financieros, beneficios, seguros, así como las tasas y toda clase de impuestos, exceptuando el Impuesto sobre el Valor Añadido que se especifica como partida independiente.

El precio de suministro será fijado por los licitadores en su oferta dentro del precio señalado como máximo en la presente memoria.

12.- RÉGIMEN DE PAGOS

El plazo máximo de pago será de 30 días a contar desde la recepción de la factura, mediante transferencia bancaria a la cuenta indicada por la empresa adjudicataria.

13.- CAUSAS DE RESOLUCIÓN

No se prevé ninguna causa específica de resolución de este contrato.

14.- 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.

15.- SUBCONTRATACIÓN

No procede

16.- MODIFICACIÓN DEL CONTRATO

No procede

17.- SEGUIMIENTO DE LOS TRABAJOS OBJETO DEL CONTRATO

El seguimiento se realizará a partir de la firma del contrato y durante los tres meses de duración del proyecto.

El adjudicatario designará una persona como Responsable del Proyecto que asumirá las labores de interlocución con el Director Técnico nombrado por el equipo de investigación de la FGUA-UAH.

El seguimiento y control de los trabajos a realizar se efectuará sobre las siguientes bases:

- Seguimiento continuo y concomitante de la evolución del proyecto entre el Responsable del Proyecto por parte del adjudicatario y el Director Técnico por parte de la FGUA-UAH.

- Reuniones de seguimiento y revisiones técnicas, del Responsable del Proyecto y del Director Técnico o personas en quien deleguen, al objeto de revisar el grado de fiabilidad del software solicitado, su ajuste a las especificaciones funcionales y la aceptación de las actividades realizadas.

- Tras las revisiones técnicas se levantará acta con el resultado de la validación de las actividades realizadas. Corresponde a la FGUA-UAH la supervisión, control y aprobación de los trabajos

18.- DOCUMENTACIÓN A PRESENTAR POR EL SELECCIONADO

Documentación técnica de los algoritmos realizados, así como el propio software.

Universidad de Alcalá

Firmado digitalmente por MARTINEZ HERRAIZ JOSE JAVIER - DNI 50704436Q
Fecha: 2022.08.10 11:22:48 +02'00'

Alcalá de Henares, 10 de agosto de 2022