

República Oriental del Uruguay

Universidad de la República

CONVENIO ESPECIFICO ENTRE LA ADMINISTRACION NACIONAL DE CORREOS Y LA FACULTAD DE INGENIERIA Encriptado y seguridad

En la ciudad de Montevideo, a los treinta días del mes de julio de mil novecientos noventa y siete, **POR UNA PARTE:** La Universidad de la República (Facultad de Ingeniería) representada por el Sr. Rector Ing. Quím. Jorge Brovetto y el Sr. Decano Dr. Ing. Rafael Guarga y **POR OTRA PARTE:** la Administración Nacional de Correos, representada por el Sr. Presidente Ing. Fernando Bracco y el Secretario General del Directorio Sr. Emilio Berriel, convienen :

Objetivos

En el Convenio Marco de Cooperación Técnica y Científica suscrito entre la Administración Nacional de Correos y la Universidad de la República suscrito con fecha 5/9/96, prevé actividades de asesoramiento y estudios especializados, que se definirán a través de convenios específicos.

A través del presente acuerdo la Facultad de Ingeniería realizará estudios y actividades para asesorar a la Administración Nacional de Correos (ANC) sobre temas de encriptado y de seguridad.

Marco de referencia

La ANC necesita usar comunicaciones de tipo electrónico para su propia administración o para prestar servicios de correo híbrido. Para que este uso sea compatible con el modo de operación de una Administración de Correos se debe garantizar la privacidad de la comunicación, así como la autenticidad del remitente en forma tal que resulte documentable. Por estos motivos está interesada en llevar a cabo estudios sobre métodos de encriptado y de firma electrónica. Asimismo está interesada en la definición de procedimientos para administrar sistemas electrónicos seguros. Los estudios objeto de este acuerdo deben permitir tomar decisiones sobre los métodos a utilizar.

El uso de sistemas de claves públicas y privadas hace necesaria la certificación. De esta manera se habilita el uso de redes de datos (en particular Internet) para aplicaciones de tipo comercial o simplemente privado. La ANC desea definir y especificar esa función, así como estudiar y cuantificar los recursos necesarios para en definitiva formular un proyecto en este sentido. Los estudios necesarios para pre formular este proyecto son no sólo los métodos de encriptado sino además los de seguridad, en particular procedimientos.

Actividades

El presente acuerdo comprenderá las actividades que siguen:

1. Estudio comparativo de algoritmos de encriptado. Seguridad que ofrecen. Complejidad de la implementación. Para los algoritmos más importantes, compromisos entre largo de la clave y seguridad. Este estudio se consignará en un informe.
2. Compatibilidad de los algoritmos con lo que usan otras Administraciones.
3. Evaluación de productos existentes
4. Especificación de las funciones y el funcionamiento de la función de certificación.
5. Dimensionamiento de recursos humanos y materiales. Especificación primaria de la red de comunicaciones necesaria.
6. Descripción de procedimientos. Se incluye la especificación de la información que se almacena, los sistemas de distribución de claves.
Si el avance de los trabajos lo justifica, se encarará la actividad :
7. Implementación de un paquete software de encriptado. Realizará la generación de claves o complementaría programas de mail existentes para mejorar la seguridad.

Metodología

Se estudiarán en forma teórica diversos algoritmos y se entregará un informe descriptivo de los mismos, en que se evaluará la capacidad de protección de los distintos algoritmos. Para algunos de ellos, presumiblemente DES y RSA, se analizará en detalle los largos de clave necesarios.

La ANC suministrará datos sobre los métodos de encriptado usados por otras Administraciones de Correos. A partir de ellos se estudiará la compatibilidad de los algoritmos estudiados con los sistemas en uso.

Se examinará en forma comparativa los productos más importantes existentes en el mercado compatibles con los que usan otras administraciones.

Se elaborará en conjunto con personal de la ANC un proyecto de prefactibilidad sobre el establecimiento de la certificación. El proyecto debe servir para evaluar la posibilidad de utilizar la transferencia de documentos o de fondos en forma segura y documentable. La participación de técnicos de la ANC es especialmente importante en cuanto a los aspectos legales de la certificación y en cuanto a la cuantificación de los recursos humanos necesarios.



Handwritten marks on the left margin: a checkmark, the number '2', a signature 'JMB' in a circle, and a large signature 'Fernando' at the bottom.

República Oriental del Uruguay
Universidad de la República

Se definirá los procedimientos de distribución de claves y se especificará una red de comunicaciones, teniendo en cuenta varias alternativas. La ANC participará en esta actividad para llegar a una definición clara de cuáles son las funciones que aspira a cubrir. Participará además en una estimación primaria del mercado, que determina el número de usuarios para el proyecto.

Se designa como coordinadora del proyecto a la Prof. Ing. María Simon, docente del Instituto de Ingeniería Eléctrica.

Etapas y entregas

1. Estudio de algoritmos de encriptado. *Mes 2*
2. Compatibilidad con otras administraciones. *Mes 3*. El informe sobre compatibilidad estará sujeto a la disponibilidad de información sobre otras administraciones, que será suministrada por la ANC.
3. Proyecto de prefactibilidad que permita evaluar y dimensionar las tareas de certificación, incluyendo recursos a invertir y opciones técnicas principales. *Mes 4*
4. Evaluación de productos. *Mes 6*
5. Descripción de procedimientos. *Mes 8*

Plazos y costos

El estudio se realizará en un plazo de ocho meses a partir del primer pago, y tendrá un costo total de U\$S 40.000 (cuarenta mil dólares americanos), a pagar en tres entregas: 15.000 U\$S a la realización del acuerdo, 15.000 U\$S a los cuatro meses y 10.000 U\$S a la entrega final.

La realización de un paquete software de encriptado - desencriptado, o la programación de capacidades adicionales para paquetes existentes usados en el intercambio de información, se pactará independientemente, si existe interés de la ANC.

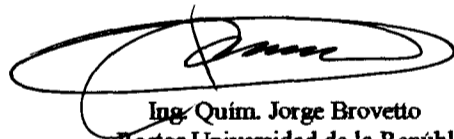
Modificaciones

De común acuerdo entre las partes podrán introducirse modificaciones al presente convenio, incluso con respecto a sus objetivos y duración, con la aprobación de las autoridades respectivas.

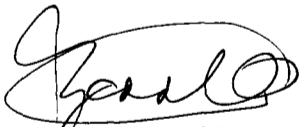
En prueba de conformidad se firman dos originales del mismo tenor, en el lugar y fecha arriba indicados.



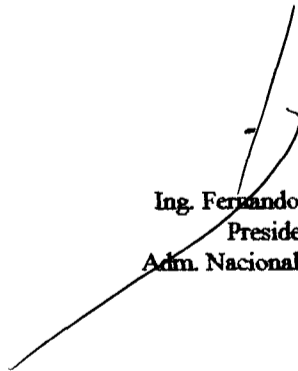
Dr. Ing. Rafael Guarga
Decano Facultad de Ingeniería



Ing. Quím. Jorge Brovotto
Rector Universidad de la República



Sr. Emilio Berriel
Secretario General de Directorio
Adm. Nacional de Correos



Ing. Fernando Bracco
Presidente
Adm. Nacional de Correos