CONVENIO ESPECIFICO ENTRE LA ADMINISTRACION NACIONAL DE CORREOS Y LA FACULTAD DE INGENIERIA

Implementación de una Autoridad de Certificación

En la ciudad de Montevideo, a los 3 días del mes de junio de mil novecientos noventa y nueve, por una parte: La Universidad de la República (Facultad de Ingeniería, en adelante la FI) representada por el Sr. Rector Dr. Ing. Rafael Guarga y la Sra. Decana de la Facultad de Ingeniería Prof. María Simon y por otra parte: la Administración Nacional de Correos (en adelante la ANC), representada por el Sr. Presidente, Dr Carlos Rocca y el Sr. Secretario General, Dr Mario Jubín, convienen :

Antecedentes

Con fecha 30 de julio de 1997 se suscribió un Convenio Marco entre la Administración Nacional de Correos y la Universidad de la República que establece la voluntad de cooperación técnica y científica, que se sustanciaría por medio de convenios específicos.

En esa misma fecha se suscribió un convenio específico sobre ``Encriptado y Seguridad" en el cual se estudiaron los fundamentos teóricos y prácticos de las técnicas actuales de intercambio, firma y autentificación de información. También se establecieron los requerimientos que deberían cumplir los sistemas a integrar para la puesta en servicio de una Autoridad de Certificación.

Actualmente la ANC está en la fase de implementación de la autoridad, en la cual, a través del presente Convenio, actuará la Universidad.

Marco de referencia

La ANC necesita usar comunicaciones de tipo electrónico para su propia administración o para prestar servicios a terceros. Ha adquirido un sistema informático que la habilita para el cumplimiento de esta función.

Objetivos

Por el presente Convenio, la ANC y la FI, desarrollarán las siguientes actividades.

. Clasificación de los tipos de clientes y de los niveles de seguridad. Preliminarmente, se enfocan tres tipos de clientes: Servidores (hosts), Usuarios que requieren identificación y Empresas. A su vez se prevée tres niveles de seguridad, asociados a la longitud de las claves y a la calidad impuesta en su generación.

Se definirán las opciones aconsejadas para distintas necesidades.

. Definición de las Prácticas de Certificación. Estas prácticas establecen el modo de operación de la Autoridad y los compromisos que ésta adquiere con sus usuarios y con otras autoridades que la reconocen como tal. Establecen también las prácticas a seguir por parte de los usuarios.

Se definirán entonces normas y procedimientos, forma de atención a los clientes, requerimientos sobre la generación de claves y otros aspectos que hacen a la operación y a la confiabilidad.

Se definirán prácticas de certificación para los distintos tipos de clientes (servidor, identificación y empresa) y para los distintos niveles de seguridad, pues una mayor seguridad en la clave debe ir asociada a los procedimientos seguidos.

. Análisis de la posibilidad de certificación internacional, en principio de alcance en el Mercosur.

. Estudio de las prácticas usuales y acordes al estado del conocimiento para el acceso en línea a las listas de revocación. Propuesta de prácticas a seguir en el caso de la ANC y sus clientes.

Para cada uno de estos item se elaborará un informe que servirá como definición de prácticas a seguir por parte de la ANC.

Metodología

Se trabajará en conjunto con técnicos de la ANC, entre los cuales se incluirán asesores legales. El equipo se reunirá al menos semanalmente.

La ANC proveerá información sobre las prácticas seguidas por otras Administraciones y por la Unión Postal Universal.

Por parte de la FI intervendrán docentes del Instituto de Matemática y Estadística y del Instituto de Ingeniería Eléctrica.

Plazos y Costos

Los trabajos dentro del presente Convenio Específico tendrán una duración de 10 meses a partir de su firma y de su aprobación por parte del Tribunal de Cuentas.

El presente Convenio tendrá un costo de USD 34.000 (treinta y cuatro mil dólares estadounidenses). Se aportarán USD 5.000 a la firma, USD 5.000 a la entrega del informe sobre acceso a listas de revocación (etapa 3), USD 14.000 a la entrega de las CPS para servidores e identificación completas (etapa 4) y USD 10.000 a la entrega de los informes finales de la última etapa (5).

Etapas

1) Al mes 2 se entregará un informe sobre los tipos de certificados y los niveles de seguridad asociados a las claves y sobre su aplicación a distintos casos.

2) Al mes 3 se entregará una versión de las CPS que permita implementar las prácticas de certificación para los casos servidores e identificación en el nivel de seguridad básico (clave más corta).

3) Al mes 5 se entregará el informe sobre el acceso en línea a las listas de revocación.

4) Al mes 9 se entregará una versión de las CPS que cubra los casos de servidores e identificación para los niveles de seguridad medio y extremo.

5) Al mes 11 se entregarán las CPS para empresas.

Modificaciones y Ampliaciones

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 particular, se requeriría la participación de la Universidad como entidad auditora del sistema de certificación.

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

Por Facultad de Ingeniería

Ing. Rafael Guarga
Rector

Prof. María Simon
Decana

Por Administración Nacional de Correos

Dr Carlos Rocca
Presidente

Dr. Mario Jubín
Secretario General