ACEPTA: Nuevo sistema de correo electrónico certificado

ACEPTA: New System of Certificated Electronic Mail

J. Dávila y J. Lázaro

Resumen

El servicio ACEPTA permite que dos interlocutores intercambien un objeto digital cifrado y autenticado. Al final del proceso se han generado las pruebas suficientes para demostrar que dicho objeto fue generado por el remitente en un determinado instante y que el destinatario lo recibió en un momento posterior. Para ello es necesaria la intervención de una tercera parte confiable, el Agente de Entrega (DS) quien será el encargado de generar las pruebas que demuestren que el objeto digital fue recogido por el destinatario; sin embargo, el DS desconoce el contenido de lo intercambiado entre los comunicantes y no dispone de información suficiente para interceptar el envío.

Todos los agentes del sistema están provistos de una identidad digital X.509v3, por lo que todos están capacitados para firmar digitalmente documentos y para recibir mensajes cifrados dirigidos a ellos. Los mensajes intercambiados irán cifrados y firmados digitalmente por el autor de dicho mensaje.

Palabras clave: Correo electrónico certificado, acuse de recibo, cifrado y firma digital.

Summary

The service called ACEPTA allows two interlocutors to interchange a cipher, authenticated digital object. At the end of the process it had generated sufficient tests to demonstrate that this object was generated by the sender in a certain moment and that the addressee received it a while later. The intervention of a third trust part, the Delivery Agent is needed. This one will generate the tests that prove that the digital object was gathered by the addressee; nevertheless, the DS neither knows the content of the interchanged thing between the communicants nor has enough information to intercept the shipment. All agents involved are provided with a digital identity X.509v3, so that they are enabled to digitally sign documents or to receive ciphered messages. The interchanged messages will be digitally signed and ciphered by the author of this message.

Keywords: Certificated e-mail, receipt acknoledgment, ciphering and digital signature.

El servicio ACEPTA permite que dos interlocutores intercambien un objeto digital cifrado y autenticado

ACEPTA es un nuevo sistema de correo certificado desarrollado íntegramente en CriptoLab, el Laboratorio de Criptología de la Facultad de Informática de la UPM (http://tirnanog.ls.fi.upm.es).

Los objetivos de este proyecto son desarrollar una aplicación independiente de la plataforma que la ejecute y que permita el envío y entrega de cualesquiera objetos digitales cifrados y firmados. La principal función del sistema ACEPTA es generar pruebas públicamente válidas del envío y de su recepción a través de acuses de envío y recibo. Todos los mensajes intercambiados en este sistema lo hacen en forma cifrada y autenticada.

El Agente de Entrega es el testigo que intermedia entre el remitente y el destinatario. Entre todos generan pruebas suficientes de que cierta transferencia se inició en un determinado instante y se completó en otro posterior, así como las identidades de todos los participantes en el proceso. El protocolo ACEPTA no permite al Agente de Entrega conocimiento alguno sobre el contenido de lo intercambiado entre los comunicantes ni disponer de información suficiente para interceptar el envío. Además, el transporte del objeto intercambiado es ajeno a las actividades propias del Agente de Entrega y éste es independiente de él.

En este protocolo intervienen diversos actores como son: el Remitente, el Destinatario, el Agente de Entrega y el Servidor de Sellos de Tiempo. Todos ellos están provistos de su identidad digital en forma de pares de claves pública/privada y de certificados X.509v3. Estas identidades son las que les permiten firmar digitalmente documentos y recibir mensajes cifrados dirigidos a ellos.

El proceso de transferencia entre Remitente y Destinatario se basa en que el Remitente cifra el objeto digital o mensaje que desea enviar bajo el control de dos claves elegidas por él al azar

El Remitente es quien inicia el protocolo y emite el mensaje. Su función es generar el mensaje, contactar con un Agente de Entrega y suministrarle pruebas indirectas de lo que se envía y, por último hacer llegar el mensaje objeto de la comunicación al Destinatario final.

A continuación el Destinatario recibe un mensaje ACEPTA mandado por el Remitente. Dentro de este mensaje está el objeto digital enviado pero, para poder abrirlo, necesita ponerse en contacto con el Agente de Entrega. El Destinatario debe demostrarle que realmente posee el mensaje para que el Agente de entrega le facilite la información que necesita para abrirlo.

La función del Agente de Entrega es la de recibir las peticiones de envío del Remitente y con ellas generar pruebas para demostrar que se ha iniciado el envío de un objeto a un determinado Destinatario. En una segunda fase, se encarga de comprobar que el Destinatario realmente posee el mensaje y le facilita su acceso definitivo.

Durante el proceso de generación de pruebas el Agente de Entrega requiere Sellos de Tiempo independientes, elemento que también interviene en el protocolo permitiendo demostrar que cierta información existía en un determinado momento.

El Agente de Entrega siempre actuará como servidor al que tendrán que dirigirse los diferentes clientes (Remitente o Destinatario) para completar las distintas etapas del protocolo. Todas las comunicaciones del protocolo se realizan con TCP/IP y todos los mensajes intercambiados están cifrados y firmados por sus autores.

El proceso de transferencia entre Remitente y Destinatario se basa en que el Remitente cifra el objeto digital o mensaje que desea enviar bajo el control de dos claves elegidas por él al azar, k1 y k2, que serán cada una de ellas una mitad de la clave efectiva de cifrado. La adecuada combinación de estas dos claves regenera la clave efectiva de cifrado con la que protege la entrega del mensaje. Una de las claves la guarda el agente de Entrega y la otra se envía directamente al Destinatario. Con esta división de secretos, el Agente de Entrega no dispone de información suficiente para, en el caso de interceptar el envío, poder abrirlo y conocer su contenido.

El transporte del objeto intercambiado es independiente de las actividades del Agente de Entrega. Este transporte podría darse por FTP o descarga desde un servidor Web, intercambio de CD o DVDs, correo electrónico, mensajería instantánea o cualquier otro mecanismo que se nos ocurra.

Una parte esencial del protocolo es la generación y entrega de las pruebas de posesión del mensaje cifrado por parte del Remitente y el Destinatario. Con estas pruebas uno de los actores del sistema demuestra que posee un determinado objeto digital y consisten en una lista de pares valor HMAC y su clave correspondiente, que le servirán al Agente de Entrega para verificar a ciegas que alguien posee el mensaje. El Agente de Entrega no necesita conocer el mensaje, sólo comprueba si las pruebas de posesión declaradas por el Destinatario coinciden con las que le entregó el Remitente.

En la comunicación entre agentes el Remitente sólo transmite la media clave, k2, al Agente de Entrega, y el mensaje junto con la media clave k1 al Destinatario. A continuación, el Destinatario tiene que demostrar ante el Agente de Entrega que posee el mensaje para que éste le facilite la media clave que le falta (k2). Estas demostraciones se basan en la lista de pares HMAC clave que genera el Remitente y que guarda el Agente de Entrega. La entrega de pruebas de posesión forma parte de varios mensajes del protocolo que van firmados por sus autores y a los que se les añade el sello de tiempo que proporciona el Servidor de Sello de Tiempos.

El protocolo completo se realiza en los siguientes pasos:

El Remitente cifra el mensaje con la clave efectiva y la divide en sus dos componentes. Una vez que tiene el mensaje cifrado, el Remitente genera la lista de pruebas de posesión y se pone en contacto con un Agente de Entrega para actuar como testigo de la transferencia. Genera una Nota de Envío y se la entrega al Agente de Entrega. La Nota contiene toda la información necesaria para realizar el envío, e identifica plenamente al Remitente y al Destinatario al mismo tiempo que incorpora la lista de pares de valores HMAC-clave y contiene la mitad k2 de la clave.

Una vez iniciado el envío, el Agente de Entrega solicita un Sello de Tiempo de la Nota y con esto obtiene pruebas independientes de que se contrató el envío en ese determinado momento.

Con toda esta información, el Agente de Entrega genera una Nota de Envío Extendida que contiene la firma del Agente de Entrega, el sello de Tiempo y una Nota de Depósito. Esta última contiene la información que necesita el Destinatario para localizar al Agente de Entrega que custodia la mitad k2 de la clave que abrirá el mensaje que recibirá. En este punto el Remitente ya posee la prueba de haber contratado un envío certificado a través de la Nota de Envío Extendida firmada por el Agente y con su Sello de Tiempo.

A continuación el Remitente manda al Destinatario el mensaje cifrado, la Nota de Depósito y la mitad de clave efectiva de cifrado k1. Este envío es independiente del protocolo, si bien todo ello se envía protegido mediante cifrado con la clave pública del Destinatario.

Una vez recibido el mensaje y abierto con su clave privada, el Destinatario utiliza la Nota de Depósito para ponerse en contacto con el Agente de Entrega y obtener la mitad de la clave k2. El Agente de Entrega reconoce a qué mensaje se refiere la solicitud y reta al destinatario a que demuestre que posee el mensaje calculando los valores HMAC para la lista de claves seleccionados por el Remitente. Con la lista de claves y el mensaje, el Destinatario puede generar la lista de valores HMAC que le devuelve al Agente de Entrega debidamente firmado. Éste comprueba que coinciden los valores HMAC con los declarados por el Remitente y, si todo va bien, queda convencido de que el Destinatario realmente posee el mensaje enviado. Con estas pruebas el Agente de Entrega solicita un Sello de Tiempo para demostrar que el Destinatario posee el mensaje en ese determinado momento.

En este punto se facilita al Destinatario la Nota de Entrega Extendida, su Sello de Tiempo y la firma del Agente de Entrega junto con la mitad k2 de la clave. El protocolo termina aquí y el ya Destinatario puede abrir el mensaje habiendo generado pruebas públicamente verificables de que posee el mensaje que le ha enviado el Remitente.

Que el Destinatario ahora decida leer o sea capaz de comprender el contenido del mensaje es algo que no atañe a este protocolo. Lo que sí se ha probado es que la transferencia se ha realizado y que nada impide que el destinatario tenga acceso exactamente al mismo mensaje que el Remitente le envió.

En este proceso se han generado pruebas tanto del envío como de la recepción del mensaje. Las primeras están en la Nota de Envío Extendida que contiene las pruebas de posesión del mensaje y su Sello de Tiempo y las de la recepción en la Nota de Entrega Extendida, que también contiene las mismas pruebas de posesión generadas por el Destinatario y el Sello de Tiempo. Todas estas notas extendidas están debidamente firmado por las participantes.

En CriptoLab hemos implementado un prototipo de este sistema utilizando Java para que sea multiplataforma y por ser un lenguaje que permite desarrollar prototipos de manera rápida y sencilla. La elección del lenguaje Java puede ser adecuada para los clientes del sistema ACEPTA, si bien no es el más apropiado para implementar el servicio que supone el Agente de Entrega.

La elección del lenguaje Java puede ser adecuada para los clientes del sistema ACEPTA, si bien no es el más apropiado para implementar el servicio que supone el Agente de Entrega

Mediante el sistema ACEPTA, el correo electrónico de hoy en día podría tener la misma validez legal y procedimental que el correo postal certificado ordinario que todos conocemos

Hay que destacar que la independencia de plataforma se ha visto truncada, ya que hay un problema en la máquina virtual de Java en Linux que no permite gestionar debidamente los certificados digitales de identidad X509v3. Este es un fallo que hemos denunciado y que ha sido reconocido por Sun pero que todavía no han resuelto.

El agente de Entrega se ha implementado como un servidor, y se ha lanzado como un servicio de Windows. Los mensajes que se intercambian en el protocolo se han definido en ASN.1 El coste de ejecución de todo el protocolo en un Pentium IV a 2,8 GHz con 1 GB de RAM, es de 614 ms. que van desde que se inicia el proceso por parte del Remitente hasta que el Remitente verifica que el correo ha sido entregado. Como se puede apreciar, este tiempo no representa un coste importante ya que han sido obtenido en el peor caso y teniendo en cuenta que se ejecuta en la máquina virtual de Java. Los costes se podrían reducir considerablemente utilizando otros lenguajes. Para el mismo escenario pero utilizando un Pocket PC 2002 funcionando a 200 MHz y con 32 MB de RAM, el tiempo de ejecución completa fue de 8,3 segundos.

El protocolo ACEPTA tiene muchas posibles aplicaciones especialmente útiles para la Administración Pública como la entrega de notificaciones de infracción, citaciones judiciales, avisos importantes y vinculantes, etc.

En el entorno académico, ACEPTA puede ser muy útil a la hora se presentar todo tipo de solicitudes dentro de un plazo de tiempo, tales como becas o proyectos, incluso para la entrega de prácticas, informes, expedientes o recursos administrativos.

En el ámbito privado, empresarial y comercial el sistema ACEPTA puede ser un componente muy útil en subastas, concursos para la asignación de proyectos, comunicaciones B2B, ofertas privadas, distribución de software y materiales multimedia, etc.

Mediante el sistema ACEPTA, el correo electrónico de hoy en día podría tener la misma validez legal y procedimental que el correo postal certificado ordinario que todos conocemos.

Más información y software en: http://tirnanog.ls.fi.upm.es

Jorge Dávila Muro
(jdavila@fi.upm.es)
Profesor Titular y Dtor. del CriptoLab.
Jorge Lázaro Molina
(jorge@dilmun.ls.fi.upm.es)
Dpto. de Lenguajes, Sistemas Informáticos e Ingeniería del SW.
Facultad de Informática - UPM