

Los servicios de certificación: oportunidades y retos

La definición de un marco estratégico para potenciar los servicios de certificación en España, en el contexto de Sociedad de la Información, tal como el que estamos viviendo, debe estar lógicamente sustentada en iniciativas que promuevan su desarrollo y uso. En este sentido, este artículo trata de identificar algunos de los desafíos asociados con la promoción del uso de la autenticación.

A este respecto, las iniciativas de desarrollo del mercado deberían, cuanto menos:

- Promover la adopción y uso de la autenticación electrónica por parte de empresas y usuarios.
- Fomentar la competencia e impulsar la innovación en nuevas tecnologías y aplicaciones.
- Expandir las oportunidades nacionales e internacionales para proveedores y usuarios finales de servicios de autenticación y certificación.

Posicionar la Autenticación como inversión estratégica

En primer lugar, es fundamental que las empresas comprendan que la autenticación electrónica ofrece la funcionalidad necesaria para la comunicación interactiva sobre redes abiertas.

Así, la inversión necesaria para su implantación requiere ser conceptuada como una de naturaleza estratégica, en la medida en que permitirá a las empresas permanecer competitivas. Podría ser útil, en este sentido, emprender acciones con objetivos específicos a nivel de asociaciones empresariales.

• Andrés Font

Director de Análisis y Prospectiva de la Fundación Retevisión/Auna

A la vez que esta tecnología debe ser reconocida y promovida como una inversión crítica de seguridad, las empresas necesitan entender cómo puede agregar valor a sus procesos. Específicamente, necesitan comprender cómo las técnicas de autenticación permiten nuevas aplicaciones y, de esta manera, generar nuevas fuentes de ingresos. En este sentido, los esfuerzos promocionales deberían concentrarse en posicionar a la seguridad como un *posibilitador* de nuevas oportunidades para la empresa.

Se ha cuestionado la viabilidad económica del uso de técnicas de autenticación. Algunos opinan que simplemente no hay "business case", mientras otros piensan que el "business case" aún está por consolidar. Aquellos que expresan este último punto de vista están convencidos de que muchas más empresas e individuos utilizarían el comercio electrónico si tuvieran garantías de que sus transacciones son seguras, y que, de esta forma, su generalización posibilitará el "business case".

Existen otros *inhibidores* a la inversión que necesitan también ser abordados. En las estructuras actuales de precios, el coste de desarrollo de la tecnología aparece como uno de los principales inhibidores, así como su coste de mantenimiento. En este sentido, sería importante aconsejar a las empre-

sas sobre los distintos niveles de seguridad posibles, así como recomendarles las estrategias de evolución hacia las soluciones que fueran progresivas y escalables.

Incrementar la conciencia y uso de los consumidores

Parece claro que, a corto plazo en el contexto de los usuarios individuales (y a menudo en el de las pequeñas y medianas empresas), no será fácil incrementar las tasas de adopción. Aunque los estudios de consumidores continúan indicando que la privacidad y seguridad son preocupaciones importantes, resulta también que la satisfacción de su compra o transacción *on line* depende de la "facilidad" con la que se realiza y del éxito de sus experiencias de compra preliminares. Estadísticas recientes muestran que los consumidores se sienten involucrados en alguna forma de "ejercicio de compensación" cuando llevan a cabo sus actividades *on line*. Con respecto a la privacidad, parece que un gran número de usuarios se encuentra dispuesto a intercambiar algún beneficio a cambio de permitir a las empresas acceder a cierta información personal. En cuanto a la seguridad, muchos usuarios carecen del conocimiento de las diferentes técnicas de seguridad disponibles, y aceptan así los niveles de seguridad básicos, por razones de comodidad y coste.

En este sentido, parece evidente que los consumidores deberán tener algún nivel de comprensión de la tecnología si deben entender ciertas características y compa-

rar las distintas soluciones, a fin de hacer elecciones informadas entre las ofertas de distintas Autoridades de Certificación competidoras. Habrá también necesidad de explicar la funcionalidad del "no-repudio" ofrecida por las distintas tecnologías. Las tasas actuales de transacciones repudiadas realizadas sobre redes abiertas sugieren que ésta es una alternativa que los usuarios valorarán cada vez más.

Otro de los aspectos en que los usuarios deberán ser conscientes es en el hecho que tendrán que asumir la responsabilidad de mantener segura su clave privada. Puesto que la experiencia del consumidor ha sido que siempre se espera de él que asuma una mayor obligación y responsabilidad con los avances tecnológicos, podría haber de hecho cierto escepticismo para utilizar certificados digitales. Esto sugiere que los mecanismos que faciliten el manejo de certificados y la distribución justa de responsabilidades serán importantes al respecto. Se ha entendido generalmente que los gobiernos tienen un papel en educar y darle potestad a los ciudadanos para que tomen conciencia de sus responsabilidades y su habilidad para ejercitar elecciones con respecto a su protección como consumidores.

Fomentar la competencia y la innovación

Los aspectos competitivos en los mercados electrónicos son similares a aquellos que se encuentran en los mercados tradicionales, matizados por algunas características especiales. En el entorno de los servicios de certificación y autenticación, pueden surgir aspectos relacionados con la competencia que requieran un seguimiento activo, a fin de evitar la aparición de estructuras de monopolio, o de concentración excesiva en el mercado.

Una preocupación en este sentido es que, en el contexto del comercio electrónico B2C, se pueda requerir una certificación por parte de una Autoridad de Certificación, en concreto al momento de emprender una transacción con alguna organización específica. En el ámbito del B2B, la preocupación se manifiesta con la potencial expulsión de la cadena de aprovisionamiento, en caso que no se empleen tecnologías particulares, o no utilicen los servicios de una cierta Autoridad de Certificación.

En el mercado B2C –y en ciertas implantaciones B2B– las asociaciones de usuarios han observado que las Autoridades de Certificación tienen el potencial de asumir en el futuro una posición privilegiada, al estar en posición de compilar las "huellas digitales" en cualquier actividad. Específicamente, se ha observado que las Autoridades de Certificación podrían hacer valer su poder con relación a los usuarios, simplemente en virtud de su función para emitir y revocar certificados. Así, resulta anticipar que una Autoridad de Certificación podría registrar todas aquellas transacciones realizadas por un individuo utilizando una firma digital, con las implicaciones negativas que esto tendría, en lo que respecta a la privacidad de los usuarios.

En relación a ello, se ha sugerido que podría

Es fundamental que las empresas comprendan que la autenticación electrónica ofrece la funcionalidad necesaria para la comunicación interactiva sobre redes abiertas

ser deseable que los gobiernos actuaran como "árbitros", aunque aquí hay que advertir del riesgo de que de esta forma se perjudique la innovación, erigiendo barreras artificiales de entrada, o permitiendo a los competidores incumbentes erigir barreras que pongan obstáculos a los entrantes. Existe, pues, la necesidad de asegurar que el mercado fomente la innovación y la inversión. Las acciones tomadas a tal fin, sin embargo, deberán en forma paralela evitar la formación de monopolios, de alta lesividad para la competitividad de la economía, garantizando niveles de calidad apropiados y condiciones justas para los usuarios.

Conclusiones y próximos pasos

El desafío es, por lo tanto, asegurar que las acciones tomadas desde todos los sectores sean coherentes con las tendencias mundiales en la materia, evitando que se produzcan distorsiones que resten competitividad a las empresas nacionales, y garantizando condiciones justas para los usuarios españoles.

Próximos Pasos

El diálogo entre el sector público y el privado es esencial para el progreso de la confianza de los usuarios, y será fundamental para el éxito en el desarrollo de un marco adecuado para España. Como próximo paso, por tanto, ambos sectores deberán colaborar a fin de:

- Establecer y facilitar un proceso para definir un conjunto de principios comunes basados en la realidad del mercado, aplicables a los servicios de certificación y autenticación en España.
- Planificar e implantar iniciativas estratégicas con el fin de promover el uso de técnicas de autenticación entre empresas y entre empresas y usuarios finales.

