No repudio

No repudio se refiere a un estado de negocios donde el supuesto autor de una declaración no es capaz de desafiar con éxito la validez de declaración o contrato. El término es a menudo visto en un entorno legal donde la autenticidad de una firma está siendo desafiada. En tal caso, la autenticidad se está "repudiado".

No repudio en seguridad digital

Con respecto a la seguridad digital, el significado criptologico y aplicación de los cambios de no repudio significa:

- Un servicio que proporciona pruebas de la integridad y origen de los datos.
- Una autentificación que con un alto aseguramiento pueda ser reafirmado como genuino.

Pruebas de la integridad de los datos es típicamente el más fácil de estos requerimientos para ser cumplido. Un resumen criptográfico de datos, tal como el SHA2, es usualmente suficiente para establecer que la probabilidad de que los datos sean indetectables cambie a extremadamente bajo. Incluso con esta seguridad, es todavía posible alterar los datos en transito, a través de un “hombre en el medio” o fraude electrónico. Debido a este flujo, la integridad de los datos es mejor reafirmada cuando el recipiente ya posee la información necesaria de verificación.

El método mas común de reafirmar el origen digital de los datos es a través de certificados digitales, una forma de clave de infraestructura publica, la cual firma digitalmente la pertenencia. Ello puede usar también la encriptación. El origen digital únicamente significa que el certificado o firma de los datos puede ser, con razonable certeza, confiable en ser de alguien quien posee la clave privada correspondiente al certificado firmado. Si la clave no es apropiadamente protegida por el propietario original, la falsificación digital puede llegar a ser una preocupación mayor.

Terceras partes de confianza (TTP)

Las formas en que una parte puede intentar de repudiar una firma presenta un desafió para la credibilidad de las propias firmas. El método estándar para mitigar estos riesgos es la participación de un tercero de confianza.

Los dos TTPs más comunes son analistas forenses y notarios. Un analista forense especializado en la escritura puede mirar una firma, compararla con una firma válida conocida, y hacer una valoración razonable de la legitimidad de la primera firma. Un notario proporciona un testigo cuyo trabajo es para verificar la identidad de un individuo mediante la comprobación de las credenciales de otros y fijar su certificación de que la firma es parte de quien dice ser. Además, un notario ofrece el beneficio extra de mantener registros independientes de sus transacciones, completar con el tipo de credencial comprobado y otra firma que puede ser independientemente verificado por el anterior analista forense. Por esta doble seguridad, los notarios son la forma preferida de verificación.

En el lado digital, el TTP sólo es el archivo de certificados de clave pública. Esto proporciona al beneficiario la capacidad de verificar el origen de un artículo incluso si no se ha hecho intercambio directo de la información pública. La firma digital, sin embargo, es idéntica al forense en ambos de

los usos legítimos y falsificados - si alguien posee la clave privada que puede crear una firma "real". La protección de la clave privada es la idea detrás del Departamento de Defensa los Estados Unidos en la Tarjeta de Acceso Común (CAC), que nunca permite que la clave salga de la tarjeta y por lo tanto requiere la posesión adicional de la tarjeta, además del número de identificación personal (PIN) necesario para desbloquear la tarjeta de permiso para utilizar para el cifrado y firmas digitales.