Glosario de términos

Acreditación
Proceso por el cual se verifica, ante la Autoridad Administrativa Competente, que la planta de certificación PKI cumple con los estándares internacionales contemplados en el reglamento de la Ley de Firmas y Certificados Digitales.

Algoritmo
Conjunto de operaciones y procedimientos matemáticos para resolver un problema.

Autenticación
Proceso técnico por el cual se determina la identidad de una persona que firma digitalmente.

Autoridad Administrativa Competente
Entidad designada por el Poder Ejecutivo para la fiscalización de las entidades de certificación y registro para el estado peruano. Asimismo, debe aprobar las políticas de privacidad y seguridad de las entidades de certificación y registro según los estándares internacionales. En el Perú, la Autoridad Administrativa Competente (AAC) es INDECOPI.

Centro de Acceso al Ciudadano
Locales o instituciones que sirven para el acceso del ciudadano a la realización de transacciones de gobierno electrónico.

Certificado Digital
Documento digital emitido por una entidad autorizada que vincula el par de claves con el suscriptor.

Clave Personal de Acceso (PIN)
Secuencia de caracteres numéricos que permiten el acceso a las claves privadas asociadas a los certificados digitales.

Clave privada
En un sistema de criptografía asimétrica, es aquella que se emplea para generar una firma digital sobre un mensaje de datos y es mantenida en reserva por el titular de la firma digital.

Clave pública
En un sistema de criptografía asimétrica, es aquella usada por el destinatario de un mensaje de datos para verificar la firma digital puesta en dicho mensaje y que puede ser conocida por cualquier persona.

Criptografía
Técnica para cifrar (ocultar) los datos de tal manera que un mensaje solo pueda ser entendido por las personas autorizadas.

Criptografía asimétrica

Tipo de criptografía que utiliza 2 claves para cifrar y descifrar la información, una privada (que no es conocida) y una pública, que conocen todos.

DNI electrónico (DNIe)
Es el Documento Nacional de Identidad Electrónico (DNIe) que acredita de manera presencial y no presencial la identidad de su titular y permite la firma digital de documentos electrónicos.

ECERNEP
Entidad de Certificación Nacional para el Estado Peruano. Se encarga de emitir los certificados raíz para las Entidades de Certificación para el Estado Peruano.

ECEP
Entidad de Certificación para el Estado Peruano. Cumple con las funciones y obligaciones de una Entidad de Certificación (EC) según lo indicado en el Reglamento de Firmas y Certificados Digitales.

EREP
Entidad de Registro o Verificación para el Estado Peruano. Cumple con las funciones y obligaciones de una Entidad de Registro o Verificación (ER) según lo indicado en el Reglamento de Firmas y Certificados Digitales.

Entidad de Certificación
Empresa que presta servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro o verificación.

Entidad de Registro o Verificación
Empresa encargada del levantamiento de datos, la comprobación de éstos respecto a un solicitante de certificado digital, la aceptación y autorización de las solicitudes de cancelación de certificados digitales.

Firma digital
Tipo de firma electrónica que cumple con todas las funciones de la firma manuscrita. Cumple con el principio de equivalencia funcional.

Firma electrónica
Conjunto de caracteres o símbolos que acompaña un documento electrónico y cumple con una o más funciones de la firma manuscrita.

Función Hash
Resumen del mensaje que permite verificar si los datos han sido alterados, si se cambia mínimamente el documento, el resumen cambia completamente.

Identidad Digital

Es el reconocimiento de la identidad de una persona en un medio digital (como por ejemplo Internet) a través de mecanismos tecnológicos seguros y confiables, sin necesidad de que la persona se encuentre presente físicamente.

Infraestructura de Clave Pública (PKI- Public Key Infrastructure)

Es el conjunto de hardware (equipos) y software (programas computacionales) que hacen posible la gestión de certificados y firmas digitales en un marco de seguridad y calidad tecnológica.

Infraestructura Oficial de Firma Electrónica (IOFE)

Sistema confiable, acreditado, regulado y supervisado por la Autoridad Administrativa Competente, que cuenta con instrumentos legales y técnicos que permiten generar firmas digitales y proporcionar diversos niveles de seguridad en cuanto a integridad de documentos electrónicos y la identidad del autor.

Integridad

Un documento electrónico íntegro es aquel que llega a su destino completo y sin alteraciones. Una Infraestructura de Clave Pública (PKI), preserva la integridad de los documentos permitiendo saber si han sido alterados en el trayecto entre el emisor y el receptor.

Interoperabilidad

Consiste en que un certificado digital sea compatible con diversos sistemas de PKI, sistemas operativos de las computadoras, dispositivos de almacenamiento, navegadores Web, etc. Para lograr interoperabilidad entre los diferentes fabricantes se toman en cuenta los estándares internacionales.

Lista de Certificados Cancelados

Base de datos que contiene la lista de certificados revocados, no válidos o con el plazo de vigencia vencido.

Lista de Estado de Servicio de Confianza (TSL)

Lista de confianza que incluye a los Prestadores de Servicios de Certificación acreditados y autorizados a operar en el marco de la IOFE. El propósito de la TSL es proveer de modo ordenado información del estado de los proveedores de servicios, teniendo un rol preponderante en los servicios considerados confiables (acreditados) y los proveedores supervisados por la Autoridad Administrativa Competente.

Niveles de Seguridad

Son los niveles de garantía que ofrecen las diferentes variedades de firmas digitales. La ley indica 3 niveles de seguridad medio, medio alto, y alto; el suscriptor tiene la facultad de decidir qué nivel de seguridad requiere.

No repudio

Imposibilidad de una persona de rechazar sus actos cuando ha plasmado su voluntad en un documento y lo ha firmado de forma manuscrita o digitalmente con un certificado emitido por una Entidad de Certificación debidamente acreditada.

Persona Jurídica
Se refiere a las empresas que han sido constituidas por una o más personas naturales. Pueden ser de la Administración Pública o Entidades Privadas.

Persona Natural
Se refiere a los ciudadanos que tienen derechos y obligaciones.

Políticas de Seguridad y Privacidad
Son los documentos donde las entidades de certificación y registro indican los procedimientos y medidas de seguridad y privacidad que brindan a los suscriptores. Estos documentos deben ser aceptados por la Autoridad Administrativa Competente.

Prestador de Servicios de Certificación Digital
Según el reglamento de la Ley de Firmas y Certificados Digitales, los prestadores de servicios de certificación digital pueden adoptar cualquiera de las siguientes modalidades:
- Entidad de Certificación:
- Entidad de Registro o Verificación
- Prestador de Servicios de Valor Añadido

Prestador de Servicios de Valor Añadido
Es la entidad que se encarga de intervenir en la transmisión o envío de documentos electrónicos grabando, almacenando o conservando cualquier información que permita certificar datos de envío y recepción, fecha y hora, etc.

Principio de equivalencia funcional
Indica que la firma digital tiene la misma validez jurídica que la firma manuscrita.

PKI
Ver Infraestructura de Clave Pública

Sello de Tiempo (time stamp)
Es un servicio que se brinda como valor añadido en las transacciones, sirve para autenticar la fecha y hora exactas (según relojes atómicos muy precisos) de una comunicación.

Suscriptor
Es la persona natural responsable del uso de la clave privada a quien se le vincula un certificado digital. Si el titular del certificado fuera una persona jurídica, la responsabilidad de suscriptor recae sobre el representante legal designado por esta entidad.

Tarjeta inteligente (smart card)
En el contexto de firmas y certificados digitales, es un dispositivo de almacenamiento, del tamaño y forma de una tarjeta de crédito convencional, que cuenta con un chip criptográfico para almacenar de manera segura y confiable las claves privada y pública, los certificados digitales y otros datos.

Tercera Parte Confiable
Es la entidad, debidamente acreditada, que se encarga de generar, gestionar y entregar los certificados digitales para asegurar la identidad del suscriptor.

Titular
Es la persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital.

Token Criptográfico
En el contexto de firmas y certificados digitales, es un dispositivo de almacenamiento, que tiene una apariencia similar a una memoria USB. Igualmente significa un medio de almacenamiento seguro y confiable de las claves públicas y privadas de los certificados digitales.

TSL
Ver Lista de Estado de Servicio de Confianza

UIT (Unidad Impositiva Tributaria)
Es el indicador base a partir del cual los diferentes cobros de impuestos, multas y otros son calculados por el estado.