WEDI Secure Messaging Workgroup

Secure Messaging Terminology Glossary

05/21/2014

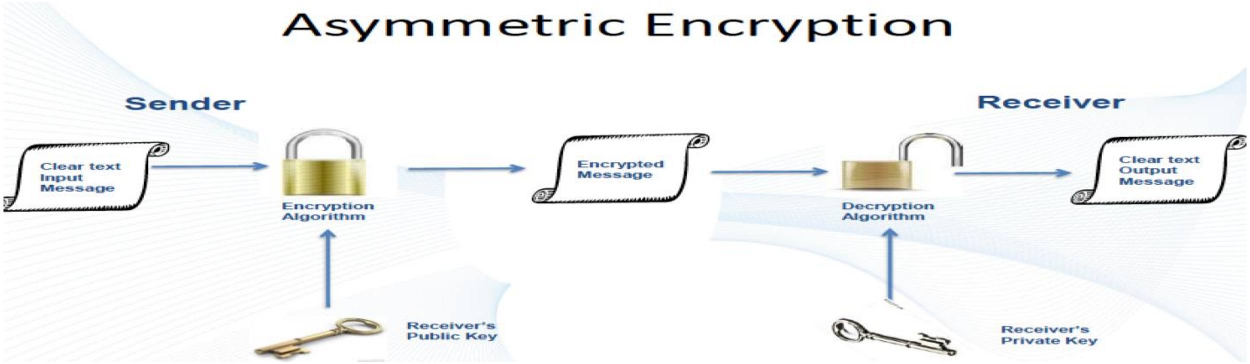
This document highlights specific terms of importance to gain an understanding of secure messaging capabilities in healthcare. It is specifically targeted to the WEDI Secure Messaging workgroup to establish a foundation of terms to use in describing various secure messaging approaches, including Direct messaging[1].

Abstract Model: The basis of the Direct Project's technical specifications, the abstract model provides a common framework for stakeholders to investigate Direct standards and services.

Algorithm: A mathematical procedure that is fed with a key to encrypt or decrypt information.

Asymmetric: One key encrypts information and different key decrypts information.

Key Cryptography: The concept of asymmetric encryption is shown in the figure below:



Certificate Authority (CA): The certificate authority issues digital certificates in a public key infrastructure environment.

Digital Signature: A fixed length hash of a document, which is encrypted with a private key, then typically sent with the original document and sender's public key (contained in a digital certificate). This method allows verification of the authorship and integrity of the message.

Direct Address: A direct address is used to identify an endpoint (a Sender or Receiver) when information is exchanged. The Direct Address has two parts, a Health End Point Name and a Health Domain Name, for example, drbob@samplehispname.org.

Direct Messaging: A Direct Project compliant messaging solution with secure email and attachments for inter-HISP communications.

DirectTrust: A voluntary, self-governing, non-profit trade alliance dedicated to the support of Direct exchange of health information, and to the growth of Direct exchange at national scale, through the establishment of policies, interoperability requirements, and business practice requirements that will enhance public confidence in privacy, security, and trust in identity. The latter, taken together, create a Security and Trust Framework for the purpose of bridging multiple communities of trust. Access http://www.directtrust.org/ for more information.

[1] Visit www.wedi.org, Privacy & Security, Healthcare Secure Messaging Subworkgroup to access 15 questions to know about Direct Messaging for more information.

Direct User or **Subscriber**: An organization or an individual that participates in sending and receiving messages and attachments using technology equipped to do so, e.g., an EHR or a web portal, via the Direct standards, and who has the authority to do so.

Federated Trust Agreement: An agreement between a trust community and its members, whereby each member attests that it has implemented and will abide by the provisions of certification/accreditation, as well as other terms and conditions associated with participation in the trust community.

Domain Name System (DNS): The DNS records tell the internet where to send the internet traffic.

Hash: A mathematical procedure that turns a message into a small number that is unique to that message.

Health Information Service Provider (HISP): A HISP is an entity that conducts the secure transmission of Direct messages to and from Direct Addresses, each of which is bound to a Direct X.509 digital certificate (i.e. provides "Direct Services"). A HISP may act in the capacity of a Business Associate or Contractor for the Customer, in which case the HISP may hold and manage PKI private keys associated with Direct digital certificates on behalf of the Customer's users/addressees.

HealtheWay or eHealth Exchange (Exchange): A group of federal agencies and non-federal organizations that came together under a common mission and purpose to improve patient care, streamline disability benefit claims, and improve public health reporting through secure, trusted, and interoperable health information exchange. Access http://healthewayinc.org/ for more information.

Individual Certificate: An X.509 certificate bound to the identity of an individual. An individual certificate is associated with exactly one Direct address, which is listed in the email Subject Alternative Name extension (preferred) or in the Email Address attribute of the Subject Distinguished Name (legacy).

Key: A secret number used to lock (encrypt) or unlock (decrypt) information.

Lightweight Directory Access Protocol (LDAP): An Internet protocol that web applications can use to look up information about those users and groups from the LDAP server.

Lightweight Directory Access Protocol (LDAP) Directory: A collection of data about users and groups.

Organizational Certificate: An X.509 certificate bound to the identity of an organization and not necessarily an individual. An Organizational Certificate is tied to a domain name by the presence of a DNS Subject Alternative Name extension that lists the domain name.

Public Key Infrastructure (PKI): The combination of software, encryption technologies, processes, and services that enable an organization to secure its communications and business transactions. The ability of a PKI to secure communications and business transactions is based on the exchange of digital certificates between authenticated users and trusted resources.

Registration Authority (RA): The registration authority establishes the identity of certificate subjects by identifying proofs certificate applicants generates certificate signing request (CSRs) for the certificate authority (CA) and is not necessarily an employee of the CA.

Relying Party: The entity that is relying on the authenticity and validity of certificates to establish trust.

Root Certificate: An X.509 certificate issued by a Root Certificate Authority and used to verify the digital signatures associated with all certificates issued by the HIDP. A root certificate is the top-most certificate of the tree structure of certificates, the private key of which is used to "sign" other certificates. A root certificate is a self-signed certificate that identifies the Root Certificate Authority. A root certificate has the X.509 CA basic constraint extension set to "true."

Secure/Multipurpose Internet Mail Extensions (S/MIME): S/MIME is an Internet standard for securing MIME data. The Direct S/MIME provides privacy and data security through encryption and authentication, integrity assurance and no-repudiation of email origin through signing.

Secure Messaging or Texting: A web-based message system that provides a drop-box like user experience for managing and exchanging encrypted, messages that may contain sensitive information with a variety of stakeholders, such as physicians and other providers, payers, nurses, members and others, .Secure messaging or texting is compliant with industry regulations such as HIPAA, GLBA and SOX. DIRECT messaging is one type of secure messaging.

SMTP: The Direct project uses Simple Mail Transport Protocol (SMTP) for email transmission. SMTP is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.

Subscriber: The subject of the certificate that often generates key pairs and must report compromised private keys.

Symmetric: The same key is used to encrypt and decrypt information. This is traditional cryptography.

Trust Anchor: Parties express trust relationships in Direct by exchanging digital.

Trust Bundle: A Trust Bundle is a collection of trust anchors from members of a Trust Community who conform to a common set of requirements set by the Community.

Trust Community: A trust community is a group of parties electing to follow a common set of standards and policies related to information exchange. A trust organization typically provides oversight and manages any supporting processes and infrastructure. Examples include DirectTrust, National Association for Trusted Exchange (NATE) – formerly Western States Consortium (WSC), SERCH, et al.

X.509 Digital Certificates: A standard for asserting that an entity is who it purports to be. The standard is strictly hierarchical, where a trusted entity asserts the identities of a set of child entities, which can make further assertions, ad infinitum.

See reference document for additional information.