PHINMS Certificate FAQs

1. What are digital certificates and what do they do?

   Digital Certificates are digital identity of a person, computer or organization. It is a binary file which is used for Authentication, Encryption, and Signature etc.
   Typically Digital certs are issued by Organizations or Root Certificate Authorities.

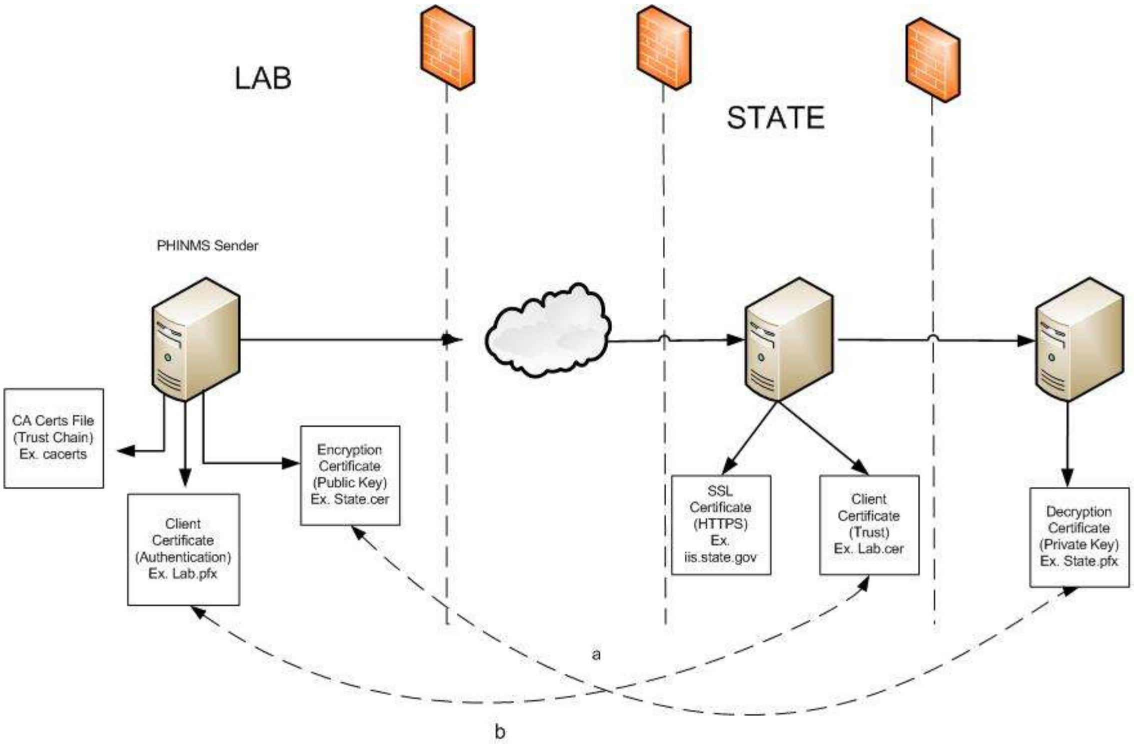
2. Is there value added when buying higher priced certificates; i.e. do higher priced certs provide more security?

   There is no concept of higher priced certificates rather encryption strength.
   PHINMS recommends 1024 bit encryption strength both on Client certificate (Sender) and SSL certificates (IIS Proxy Server).

3. Is there a recommendation related to 128 bit versus 128/256 bit SSL certificates?

   SSL Certs should be 1024 bit length.

4. What are the different types of digital certificates? Which ones are required for a sender/receiver to successfully exchange data? Specifically, what does each certificate do and why is it required?


LAB
STATE
PHINMS Sender
CA Certs File (Trust Chain) Ex. cacerts
Client Certificate (Authentication) Ex. Lab.pfx
Encryption Certificate (Public Key) Ex. State.cer
SSL Certificate (HTTPS) Ex. iis.state.gov
Client Certificate (Trust) Ex. Lab.cer
Decryption Certificate (Private Key) Ex. State.pfx
a
b

PHINMS Sender Side:

Client Certificate: For most CDC related programs this will be a CDC SDN issued digital certificate to an individual. This is used to authenticate the sender in an Organization to the receiver. Ex: sender.pfx. This certificate is a combination of both private key and public of the sender's cert.

Encryption Certificate: This is the public key of the receiver (recipient). Ex: state.cer.
This certificate can be downloaded by doing an LDAP lookup or obtaining this in an email from the receiver. This is used to encrypt the data sent to the receiver. Ex: Receiver.cer

CA Certs: CA Certs is a Key store which comes bundled with the PHINMS product. When a sender is trying to make a HTTPS (SSL) connection to the receiver IIS server, it needs to validate the certificate chain of the SSL certificate installed on the IIS server. PHINMS uses this key store to look up for trust chain.

If the Root and Intermediate cert of the SSL certificate is not present in the CA certs file then HTTPS connection fails. In order to fix this, the receiver (State) needs to provide their Root and Intermediate of the SSL certificate to the sender in an email. This needs to be imported on the sender.

PHINMS Receiver Side:

SSL Certificate: This is the certificate installed on IIS proxy server to provide HTTPS (SSL) connection to the sender. SSL connection creates a secure tunnel between Sender and the IIS server. This certificate has to be purchased from a Vendor. You can also use the existing one or generate your own using Open SSL. If you use the non popular of open source, please make sure to provide the root and the intermediate (if exists) to the sender to add to the trust chain.
Ex: state.us.gov

Client Certificate (Public Key): Client certificate on the IIS proxy server refers public key of the sender's client certificate. This is allows recipient to trust sender by providing Authentication and Authorization. This needs to be provided by the sender's side to recipient by email.
Ex: sender.cer

Decryption Certificate: For most CDC related programs this will be a CDC SDN issued digital certificate to an Individual. This is used in decrypting the data sent by sender. Ex: Receiver.pfx. This certificate is a combination of both private key and public of the sender's cert.

5. Are there vendors that PHINMS recommends more (or less) than others?

   There are many vendors which issues digital certificates like Client certificate and SSL server certificates. Some of them are Verisign, Thawte, Entrust, Equifax, Geotrust, etc. PHINMS (CDC) doesn't recommend one over other. You can also you the existing certificate and also can use self signed certificate.

6. Where are the certificates obtained? Does a state need to purchase the certificates? Can they use just the CDC SDN certificate? If they need to purchase the certificates, then where do they purchase them from (list of sources would be nice)?

   Please refer to Question No 4 and 5.

7. If the certificate expires, how does one go about getting it updated? Are there any early warnings that are provided to the certificate holders when it is about to expire (specifically for state health departments using Direct Send)?

   - If the Client certificate applies please go to https://ca.cdc.gov and apply for a new certificate. Please contact PHIN Helpdesk for further details.

     Phone: 1-800-532-9929, option 2
     Email: PHINtech@cdc.gov

   - If you have applied cert choosing either PHINMS staging or production activity, then you will get an email notifications as a reminder to re-apply for new certificate. These reminders will sent three times (1 month, 15 days and 5 days) before the expiration date of your certificate.
   - For SSL certificates please have your vendor notify you before it expires.

8. What are some of the signs that there may be a certificate problem? If a state is receiving data from the source but it is encrypted and they can't decrypt, what type of certificate problem could this be?

   There are several signs of certificate problem we come across while dealing with certificate. Some of the most common issues:
   - SSL and Client Certificate expiration
   - Encrypting with a wrong public key on the sender side
   - Issue with Sender not able to trust the receiver's SSL cert chain
   - Wrong private key password typed using the sender or receiver's console

   Easy way to troubleshoot a problem is to reading and understanding the log files.

   For further assistance, please call PHIN Helpdesk for support.
   Phone: 1-800-532-9929, option 2
   Email: PHINtech@cdc.gov