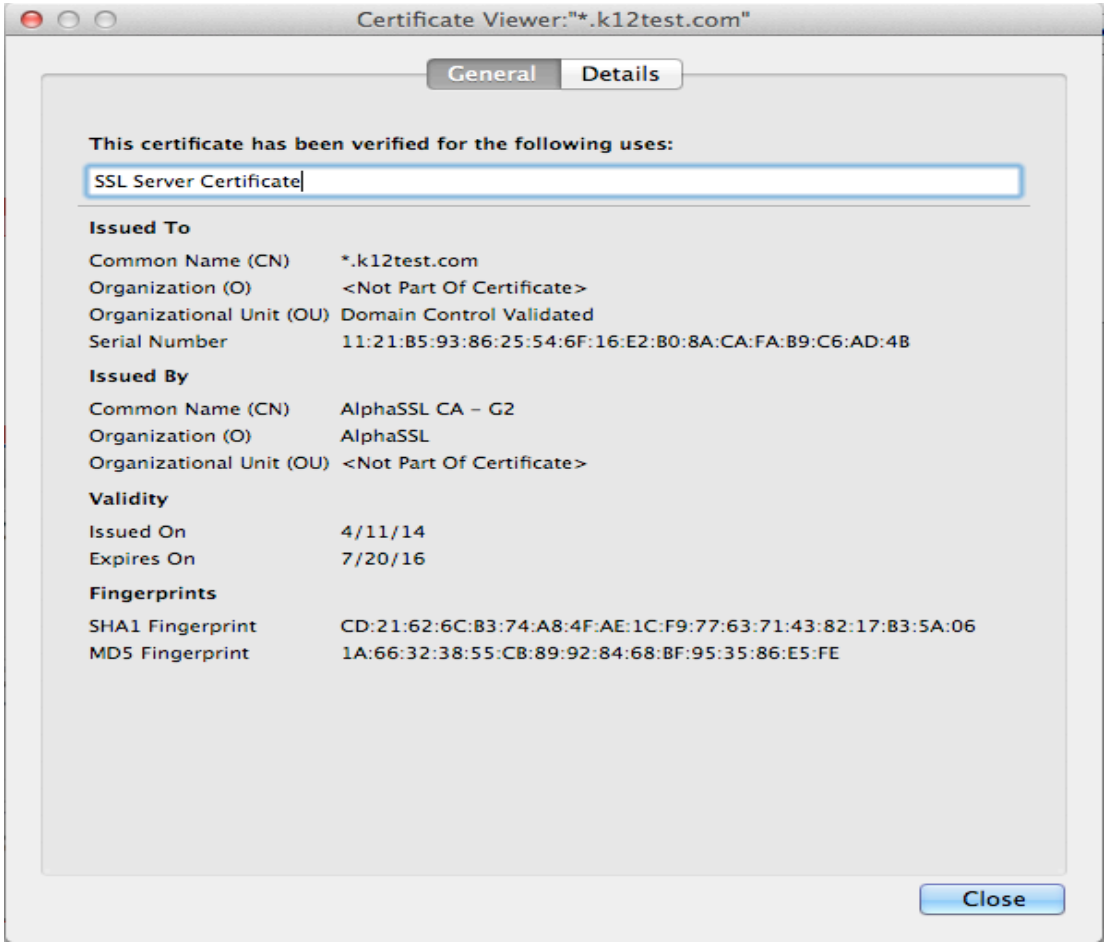
# Alaska Alternate Assessment

# Website Security Assurances

**June 2014**

**ISSUE 1: Secure access to http://ak.k12test.com**
The AK website makes use of the cryptographic protocols Transport Layer Security (TSL) and Secure Socket Layer (SSL) to provide security from each end user's computer and the website's server. In order for this to work, a public key certificate has to be installed on the web server and signed by a trusted Certificate Authority (such as VeriSign or Alpha). Web browsers connect to the website over HTTPS using port 443, and after a series of handshakes using public and private keys, a secure connection is established. Any information sent from the website to a user's computer, and vice versa, is encrypted before being sent. This ensures protection from eavesdroppers and man-in-the-middle type attacks. The Site was made secure in August 2010.

**ISSUE 2: Security of the website, the hosting servers, and transfer of secure data**
To secure the AK website, a wildcard SSL certificate was purchased (for several hundred dollars) and installed on the web server. This uses Advanced Encryption Standard (AES) 128-bit high-grade encryption - the same level of encryption used by banks. Included in this report are several attachments which verify and document the security of the website. See below:



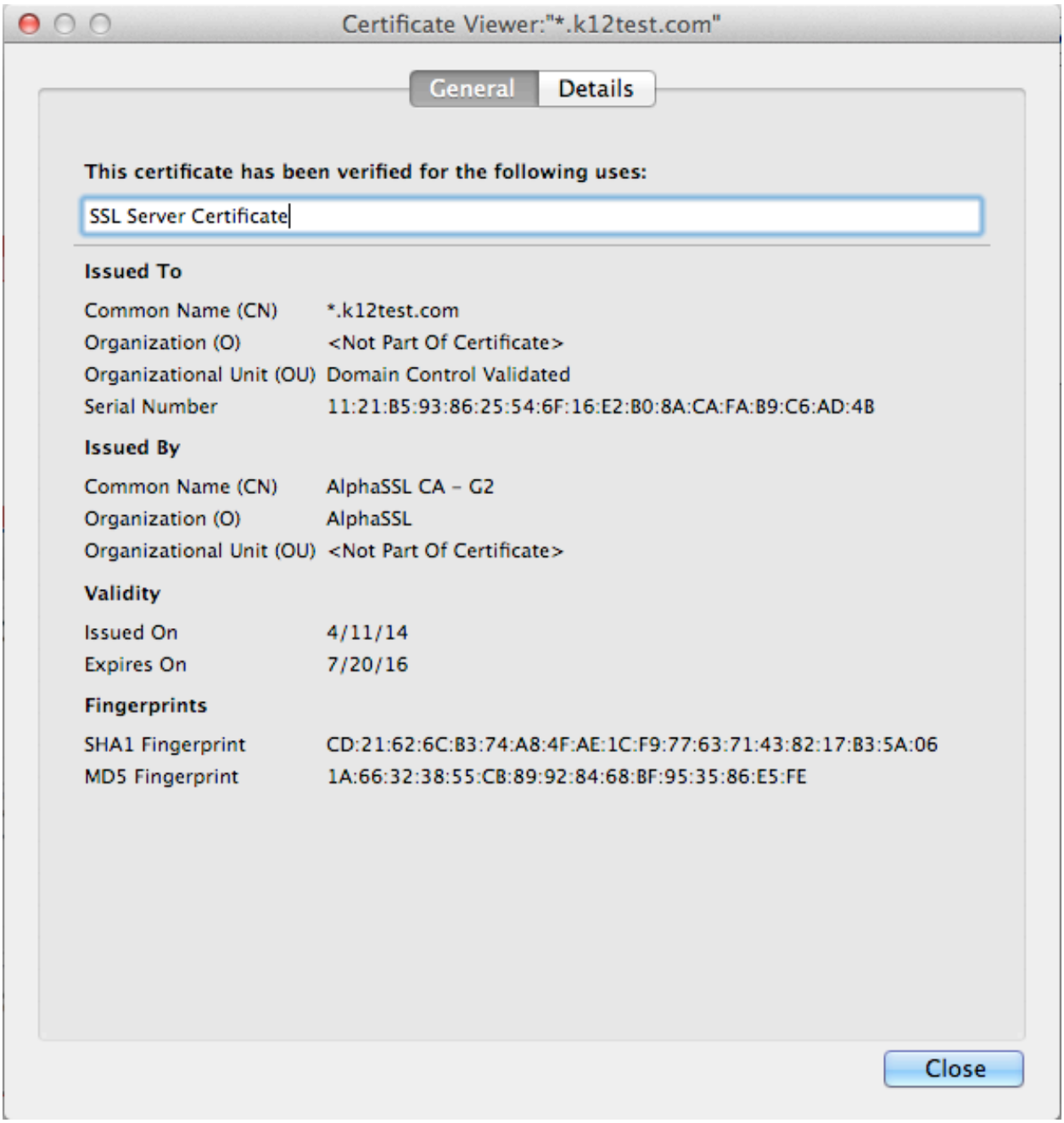
**ISSUE 3: Security of the secure transfer site (filetrans.easycbm.com)**
The Secure File Transfer Protocol (SFTP) server used for AK files (the "Fetch Server") uses a similar technology to that of the website (SSL), though it encrypts connections over port 22 instead of 443. Web servers can be configured to simultaneously listen for requests over the http:// protocol on port 80 as well as the https:// protocol on port 443, for increased compatibility with browsers, computers, and network settings. Based on previous feedback, the AK website may be configured in this fashion to ensure successful mentor trainings, so that computer settings and network filters/configurations would not hamper the trainings. As these trainings are concluded, the web server is then re-configured to force all web traffic requests to come over HTTPS.

File Transfer Protocol (FTP) servers such as our "Fetch Server" don't use http or https, but rather ftp and the secure, sftp, instead. These are similar concepts the web protocols but different implementation and port numbers. File Zilla is a popular windows SFTP client. After a connection with File Zilla is made, the "Response: fzSftp" bit can be used to verify the Sftp protocol is being used to connect. You can also view the Filla Zilla log and verify that 'open "akdoe@filetrans.easycbm.com" 22' is using port 22 (the standard port for SFTP), rather than port 21 (the port for plain FTP).

The cloud infrastructure powering the AK website and SFTP services is leased by Dillard Research Associates and hosted on commercial hardware and network connections. The highly secure data centers providing the cloud utilize state-of-the art electronic surveillance and multi-factor access control systems. All of the AK AA information is stored on redundant disk arrays, and backup system employing both frequent near line snapshots in addition to offsite weekly copies is utilized. Our systems are scanned every 5 minutes for uptime, and multiple performance metrics are captured and verified at this frequency. Basing this system in the cloud allows quick scaling and recovery options such as multiple data centers and vps configurations.

**Firefox Reporting the encrypted connection:**

**SSL Server Certificate with SHA1 and MD5 fingerprints:**



**Apache Directives enabling SSL on the server:**

```
# Enable SSL
SSLEngine on
SSLCertificateKeyFile /etc/apache2/ssl/_.k12test.com.key
SSLCertificateFile /etc/apache2/ssl/_.k12test.com.crt
SSLCertificateChainFile /etc/apache2/ssl/AlphaSSLroot.crt
```