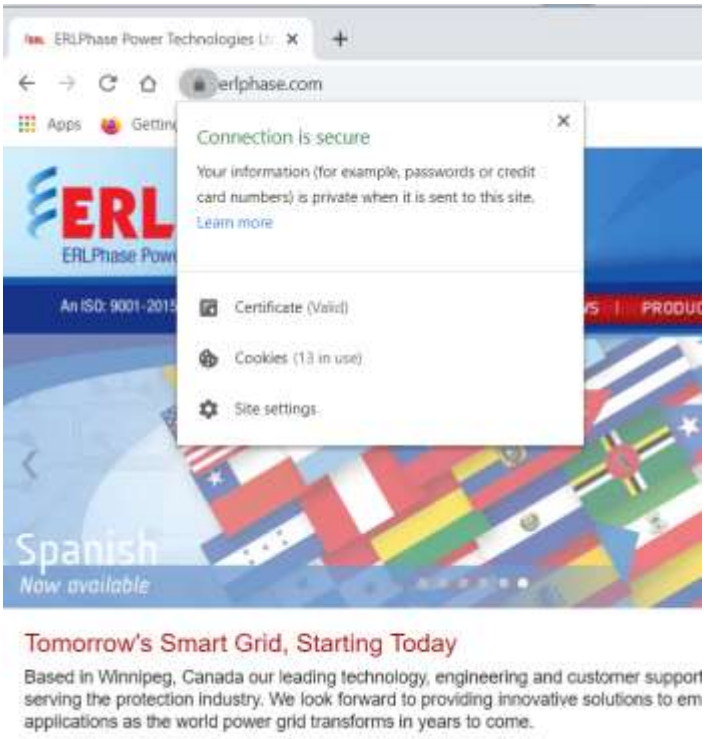
Verifying Integrity of ERLPhase Software Downloads

This note explains how end users can verify MD5 checksums and digital signatures to ensure integrity of ERLPhase software downloads.

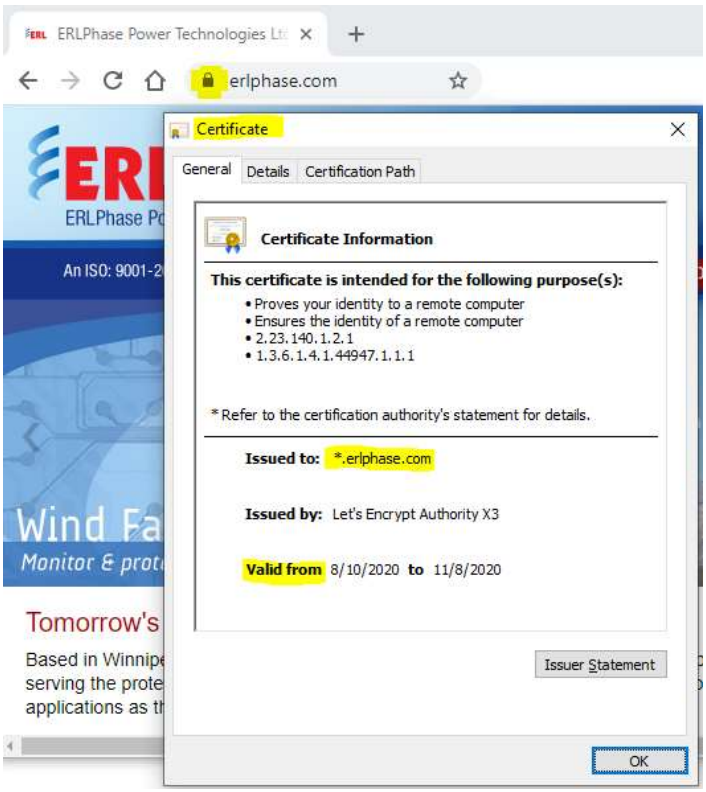
MD5 Checksums

After a file has been downloaded, use MD5 Checksum to ensure it is genuine by verifying that checksum information matches the code listed at the ERLPhase website.

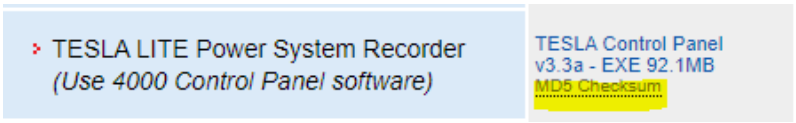
1. First, make sure you are on the correct and secure “https://” ERLPhase website by checking for a valid certificate. To view certificate validity, click on the lock beside the website URL:



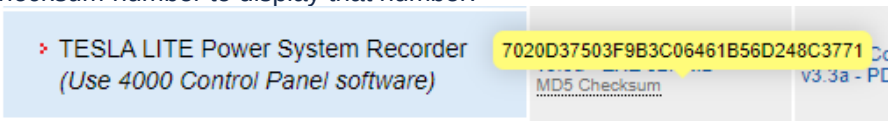
Click on *Certificate* to confirm the validly of the certificate and to view its details (as shown below).



2. At *Support* > *Software*, the text *MD5 Checksum* will show up below each software download:



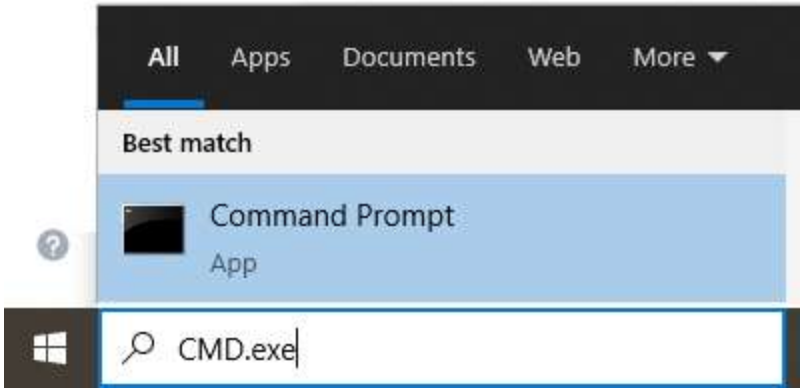
Hover over *MD5 Checksum* number to display that number:



3. After downloading the software file, use any tool to check the hash codes. In this document, we use both "CertUtil" and the website http://www.virustotal.com as examples.

Operational System: Microsoft Windows - CertUtil tool

1. Open the Command Prompt running the CMD.exe:



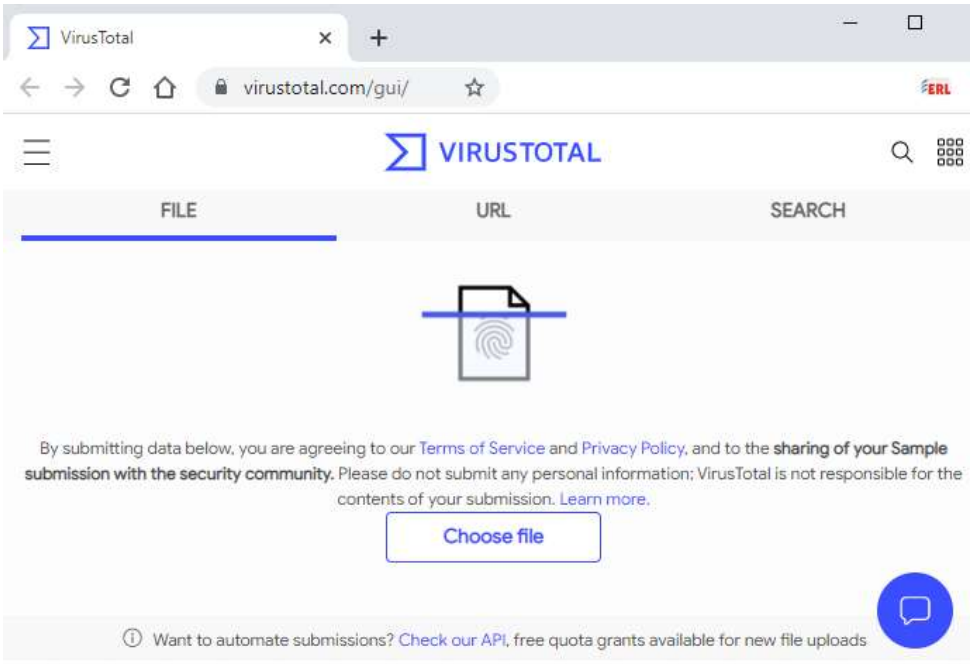
2. In the prompt command line, type the following command with the entire filename and path between “quotation marks”:

CertUtil -hashfile "C:\Users\creis\Downloads\TESLA_4000_Control_Panel_Installation.exe" MD5 as shown in the first line below and click Enter:

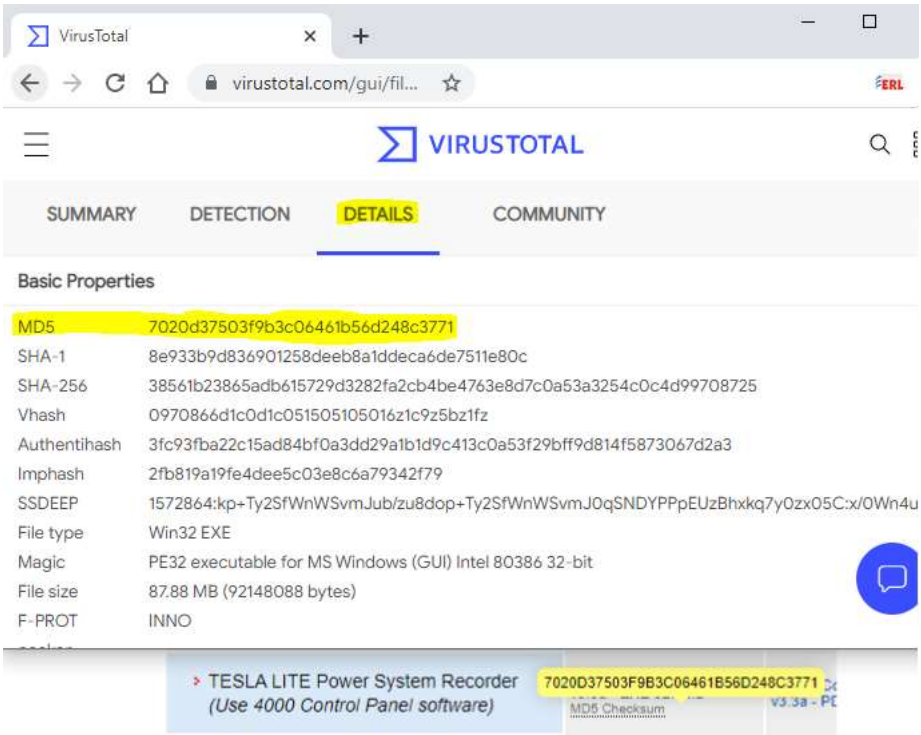
3. The following screen will display the hash code to be compared with the code on the ERLPhase website:

Website Tool: VirusTotal.com

1. Open the website to http://www.virustotal.com.



2. Click *Choose file*, then upload the file you have downloaded from the ERLPhase website and wait for the system to do the analysis. This process may take a few minutes. Once the analysis is completed, select the tab *Details*.

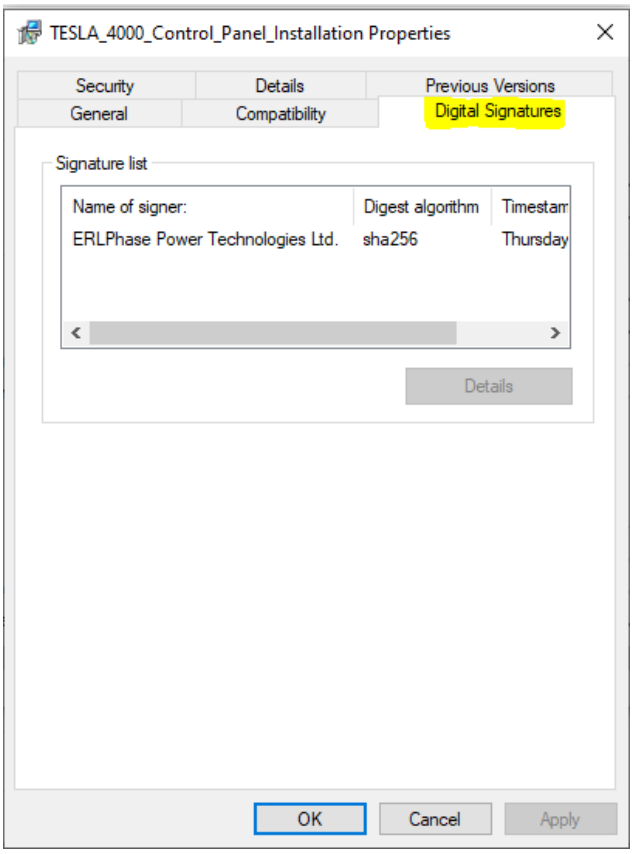


3. Compare the MD5 result under *Basic Properties* with the hash code on the ERLPhase website. Note that the alphabetic characters may not appear in capital letters as shown in the ERLPhase website, however, they should show the same alphanumeric characters.

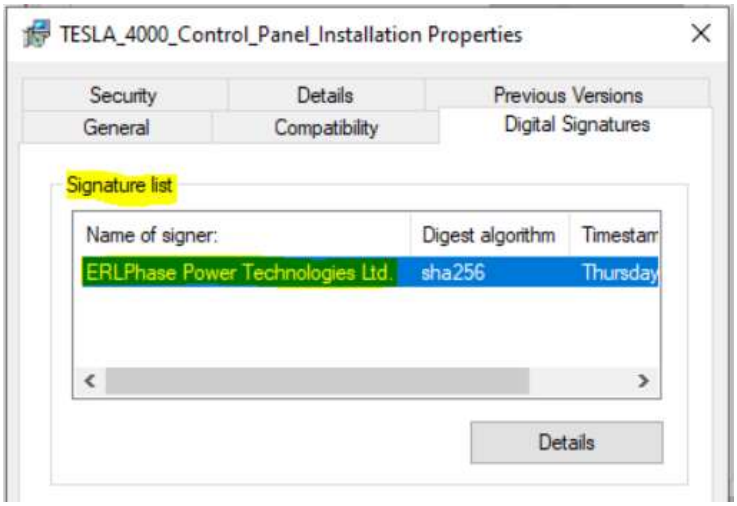
Verifying Digital Signatures on ERLPhase Software Downloads

ERLPhase uses digital signatures on our software so users can verify that their download has not been altered or tampered with. The instructions below describe how to check the digital signature on ERLPhase software that you have downloaded.

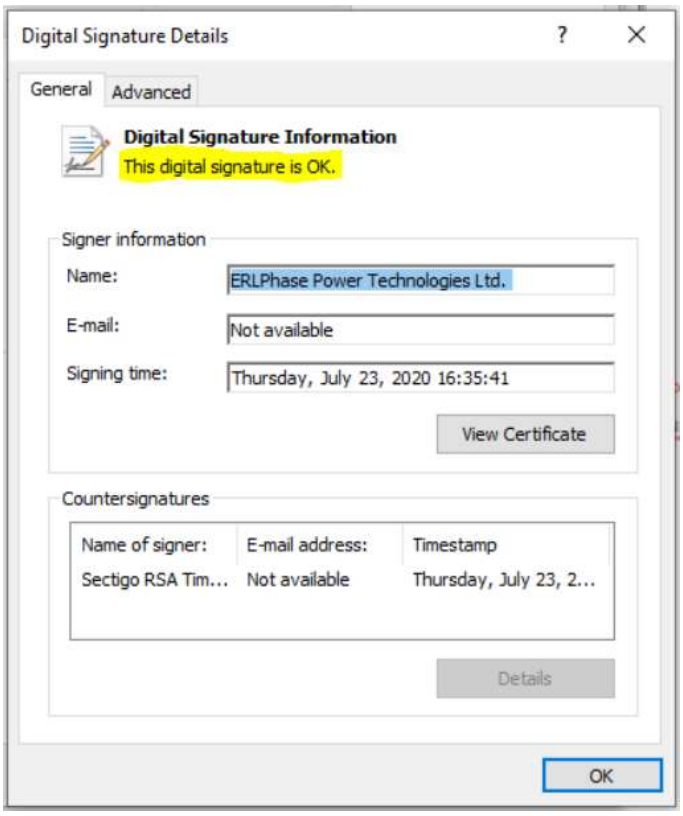
1. In Microsoft Windows, open *Windows File Explorer* and navigate to the folder containing the software file to be verified
2. Right-click the downloaded file and select *Properties*
3. Select the *Digital Signatures* tab (if you do not see a *Digital Signatures* tab, please contact support@erlphase.com for further instructions)



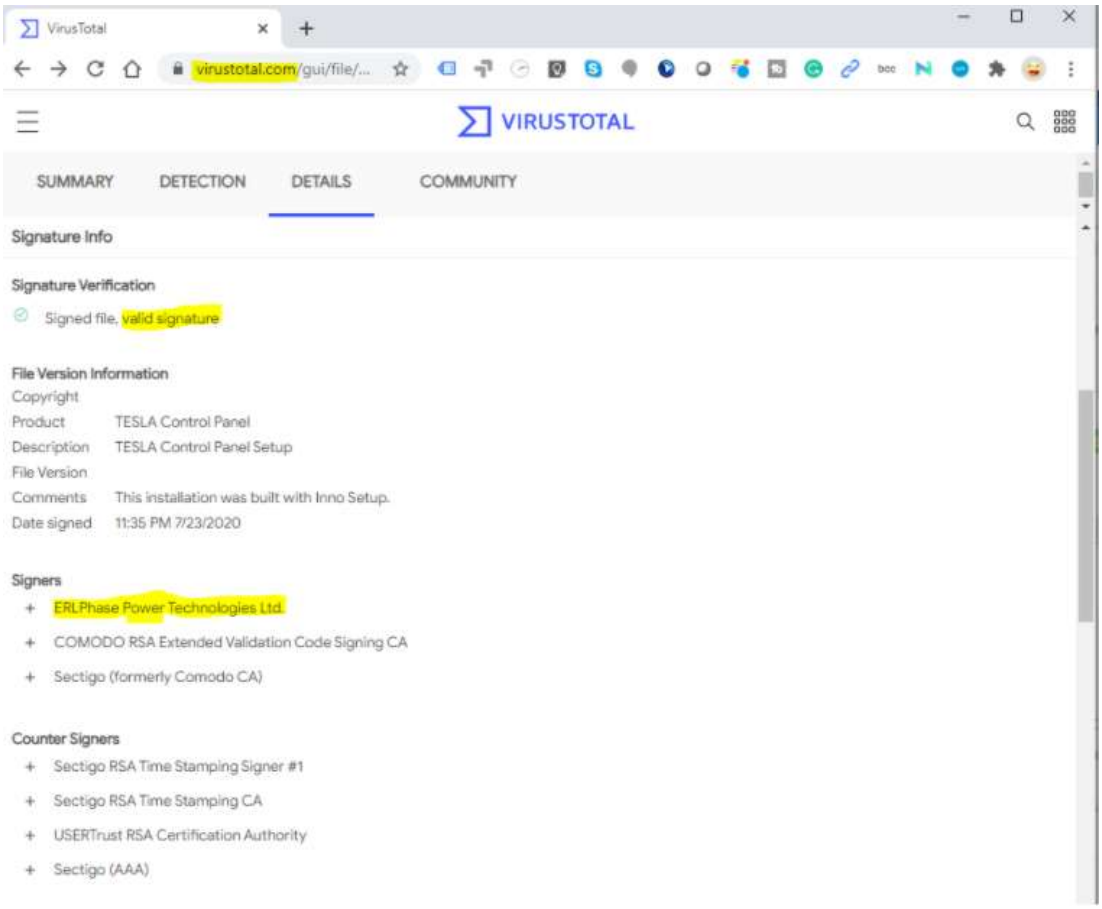
4. Click on the name of the signer in the *Signature list*



5. Click on the *Details* button
6. Verify that the *Name* in the Signer information box exactly matches the spelling "ERLPhase Power Technologies Ltd." and that the message under Digital Signature Information says, "*This digital signature is OK.*"



ERLPhase software files can be also checked by Sigcheck (offers the ability to scan the file for viruses) by submitting it to http://www.virustotal.com. Using that tool, the signature can be viewed under *Details*, then *Signature Info*, as shown:



Note: Sometimes, the Virus Total website may detect false positives, i.e. innocuous resources detected as malicious by one or more scanners. As long as the file has the ERLPhase Digital Signature tab and the correct hash codes on it, this is not a concern. If you do not see an ERLPhase Digital Signatures tab, please contact our Customer Support team.

Please contact ERLPhase Customer Support (support@erlphase.com) if you have further questions about the use of software hash codes and digital signatures to verify integrity of ERLPhase software.