Virginia Information Technologies Agency

VITA self-sign root digital certificate

The VITA self-signed root digital certificate has been made available to the public to allow any entity to verify the digital signature of an electronic message signed using a digital certificate based on the VITA self-signed root digital certificate. The VITA self-signed root digital certificate can be found at the following URL:
https://webmail.vita.virginia.gov/vita/vitaintadcapath.p7b

The Thumbprint to validate the integrity of the VITA self-signed root digital certificate is:
5E69B1C0 7E851889 C9B2E13B 731EF1AF D4719E0A (sha1)

To install the self-signed partnership root certificate on a Microsoft Windows system:

- Open the root certificate file (double click it or right click and select open)
- A window called Certificates will pop up.
- Expand the folders on the left hand pane and select the folder called Certificates
- Double click on the "VITA Internal Root CA"
- Select next until the screen prompts to finish.
- Select finish
- Repeat the process for the "VITA Internal User SubCA."

To import a certificate into Microsoft Outlook (contact list)

- In Contacts, open the contact form for the individual whose certificate you want to import
- On the Contact tab, in the Show group, click Certificates, and then click Import
- Locate and select the certificate file that you want, and then click Open.

To add a contact and certificate received in an e-mail message to your contact list

- Open the digitally signed message from the recipient.
- Right-click the name in the 'From Field', and then click 'Add to Contacts' on the shortcut menu.
- If a contact entry already exists for this person, select 'Update new information'

A digital certificate, as defined within the field of cryptography, is an electronic document which utilizes a digital signature to bind a publicly-accessible encryption key to the identity of the encryption key owner. This identity is compromised from information such as the name of the person or organization that owns the encryption key, the postal address of the entity, and the contact information for more information about the owner of the encryption key. The certificate is normally used to verify that the publicly-accessible encryption key belongs to the stated owner. A digital certificate can be used to receive encrypted email or digitally sign an electronic document.

A digital signature is simply a mathematical algorithm used to demonstrate the authenticity of a digital message or document. A valid digital signature provides the recipient a basis to believe that the message was created by a known sender and that the message was not altered in transit. Digital signatures are equivalent to traditional handwritten signatures and can provide non-repudiation as well as authentication.

A self-signed digital certificate is used strictly as an identity certificate. The self-signed digital certificate is signed solely by its creator and does not provide an independent verification for the identity of the certificate owner. The self-signed digital certificate uses a digital signature to bind a public key with the user’s identity to produce the certificate.