Puzzle of the Day

The PEM certificate hierarchy is a tree-like structure, with the Internet Policy Registration Authority as the single root. Beneath it are the Policy Certification Authorities; each PCA certificate is signed by the IPRA. The PCAs in turn sign certificates of organizational units, which sign certificates of individuals.

Suppose someone wants to verify my certificate. They will obtain the certificate of UC Davis (which signed my certificate) and use the UC Davis public key to validate my certificate. They can then validate UC Davis' certificate by obtaining the certificate of the PCA called RSADSI, which signed UC Davis' certificate; similarly, they can verify RSADSI's certificate by obtaining the certificate of the IPRA.

But how can the valdity of the certificate supposedly obtained from the IPRA be verified? How can the IPRA ensure that everyone has access to the correct certificate?