

- Filename: eccouncil-ceh31250-v11-20-4-1-public-key-infrastructure.md
 - Show Name: CEHV11 (312-50)
 - Topic Name: Cryptography - Cryptography
 - Episode Name: Public Key Infrastructure
- =====

Public Key Infrastructure

Objectives:

- Define PKI
 - Public Key Infrastructure
 - Create certs
 - Issue certs
 - Revoke certs
 - Manage certs
- PKI Components
 - [https://www.techotopia.com/index.php/An_Overview_of_Public_Key_Infrastructures_\(PKI\)](https://www.techotopia.com/index.php/An_Overview_of_Public_Key_Infrastructures_(PKI))
 - Certificate Management System (this is the software that runs the whole thing)
 - Creates Certificates
 - Certificate Distribution
 - Certificate Store
 - Certificate Verification
 - Digital Certificates
 - The actual cert
 - Used to verify entities (users)
 - Validation Authority
 - Validates digital certs
 - Does this by hosting a Certificate Revocation List (CRL) and responding to CRL requests
 - Reduces workload of the CA
 - Certificate Authority
 - Issues digital Certs
 - Validates digital certs
 - Revokes digital certs
 - Deletes certs
 - End Users
 - Request Certs
 - Manages
 - Registration Authority
 - 'pre-screens' cert signing requests for initial enrollments and renewals
 - RA verifies requester (person/org)
 - Then forwards these requests to the CA
- PKI Process

1. Subject (user/org) applies for cert from the RA
 2. RA processes the request
 - Verifies the subject's identity
 - Requests the CA to issue Public Key cert to Subject
 3. CA processes request from RA
 - Issues Cert/public key to Subject
 - An update message is sent to the VA with the Subject's info
 4. User receives cert and uses it
 - Communication is signed with cert
 5. Recipient(Client) queries the VA
 - Checks that the cert is valid
 6. VA verifies the cert
- CA Services
 - 3rd party trusted
 - Signed CA vs Self Signed
 - Hi! I'm Billy.
 - How can I verify that you're really Billy?
 - I can show you some ID.
 - OK, Let's see it.
 - Hold on while I create my ID.
 - So you're going to generate your own ID.
 - Yup!