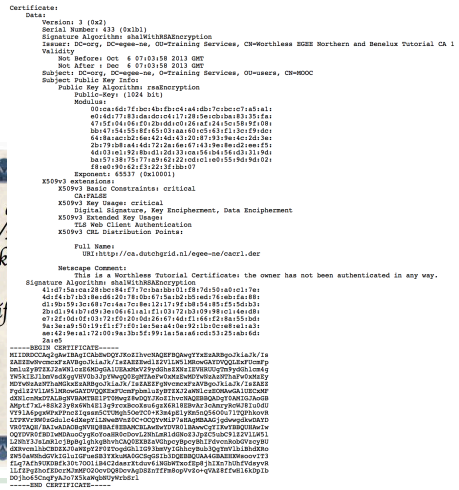
Grid Security - Extras

Security levels

- **Transport level**
  - Prevents from eavesdropping
  - Secure Socket Layer (SSL)
    - ✓ OpenSSL
    - ✓ Mutual authentication
    - ✓ Asymmetric + Symmetric encryption

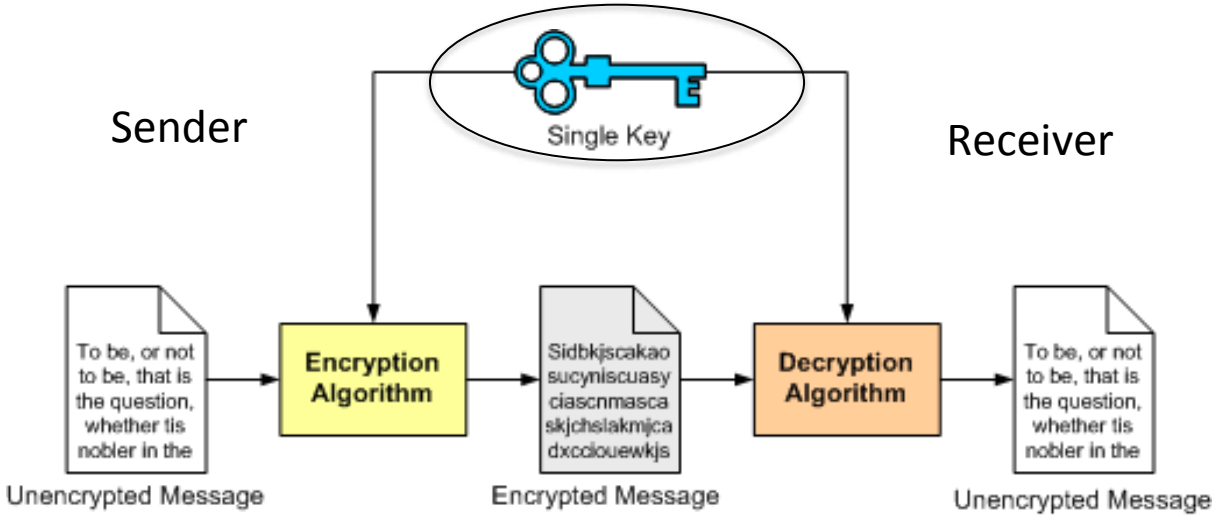
- **Message level**
  - Secures message Integrity
  - X509 certificates
    - ✓ Certificate body + Digital Signature



Encryption

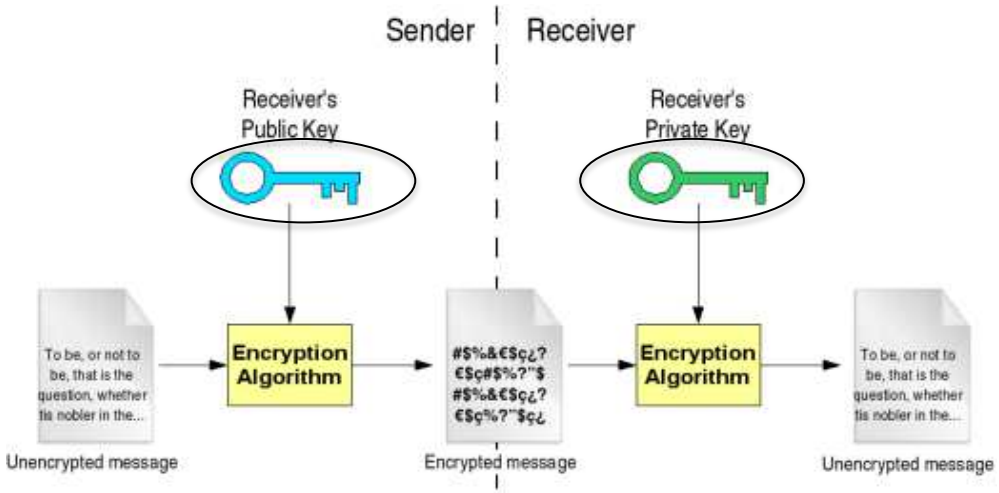
- **Types of Encryption**
  - Symmetric cryptography
    - ✓ Both sender and receiver share a common key
    - ✓ Same secret key for encryption and decryption of data
    - ✓ Short lived
    - ✓ Better performance
    - ✓ Kerberos
  - Asymmetric cryptography
    - ✓ Key pair
    - ✓ Long/short lived
    - ✓ Certificates
    - ✓ More secure
    - ✓ Computationally expensive

Symmetric keys



- Fast process
- Shared secret
- Performance
- Lacks security

Asymmetric keys



- **Data encrypted with receiver's public key can only be decrypted with his matching private key**
  - Public key - encryption key. Public via a trusted CA.
  - Private key - decryption key.
    - ✓ Secret. Known only to you.

- **Mathematic algorithm – Prime numbers**
  - practically impossible for computers to calculate the private key from the public

CA certificates – self signed

- Certification Authority (CA):
  - Confirms ID
  - Combines Id and public key
  - Calculates a hash
  - Encrypts it with CA's private key
- Who signs the CA certificate?
  - CA signs it with its own private key
  - Self-signed

CA ***FOO*** signs SURFsara's certificate

CA ***FOO*** signs its own certificate