**TOPICS:**

1. PGP Key - Extension(import and export)
2. Signing Key - Extension(import and export)
3. Security key
4. PGP generation
5. Bytes,Algorithm,Method
6. SAAS Application
7. Extensions and Naming convention
8. Extension on upload
9. Keys length

**OUTBOUND/INBOUND** : Encrypt using public key and Decrypt using private key.

Receiver only create PGP key.

**Importing Your Public Key:**

**NAVIGATION:**

Oracle HCM Cloud -> Security Manager job role or privileges ->

**Navigator** > **Tools** > **Security Console**  ->

Certificates tab ->**Import** -> **Certificate Type** to **PGP ->**

**Alias** field, enter **customer-key**.

**Browse** (location of the customer public key) ->**Import and Close** to import the public key into the Oracle HCM Cloud key store.

**Generating the PGP Encryption Key Pair:**

Oracle HCM Cloud -> Security Manager job role or privileges.

**Navigator** > **Tools** > **Security Console**  -> Certificates tab

**Generate ->** set **Certificate Type** to **PGP -> Alias** field, enter **fusion-key**.

**Passphrase** field, enter a passphrase for the private key.

(passphrase is needed when you edit, delete, or download the private key)

**forget the passphrase:**

**Key Algorithm** field, select **RSA -> Key Length** field, select either **1024** or **2048 ->** Click **Save and Close**.

**SIGNING FILE** : Sign file using private key and verify using public key.

**SIGNING KEY** : Used for verification purpose.

**THREE IMPORTANT FUNCTION DONE BY SIGNING KEY:**

* **Integrity** - A digital signature allows the recipient of a given file or message to detect whether that file or message has been modified.
* **Authentication** - A digital signature makes it possible to verify cryptographically the identity of the person who signed a given message.
* **Non-repudiation** - A digital signature prevents the sender of a message from later claiming that it did not send the message.
* Detect whether that file or message has been modified.
* Verify cryptographically person who signed a given message.

PGP GENERATION:















