School of InfoComm Technology
Taking IT Higher

NGEE ANN POLYTECHNIC

CRYPTOGRAPHY (CTG)

Diploma in Cybersecurity and Digital Forensics (Dip in CSF)

Academic Year (AY) `20/`21 – Semester 2

WEEK 6.1

DIGITAL CERTIFICATE
PRETTY GOOD PRIVACY (PGP)

Last Updated: 19/11/2020

Contents

- Recap – Cryptographic Hash Function & Digital Signature
- Digital Certificate
- Public-Key Infrastructure
- Pretty Good Privacy (PGP)
- Summary

Digital Certificate

Source: SECURITY+ GUIDE TO NETWORK SECURITY FUNDAMENTALS - 4th Edition – Mark Ciampa - Cengage Learning

Defining digital certificate

Managing digital certificates

Types of digital certificates

X.509 digital certificate standard

Knowledge Component

Defining Digital Certificate

- Trusted third party
  - Used to help solve the problem of verifying identity
  - Verifies the owner and that the public key belongs to that owner
  - Helps prevent man-in-the-middle attack that impersonates owner of public key
- Information contained in a digital certificate
  - Owner's name or alias
  - Owner's public key
  - Issuer's name

Defining Digital Certificate

- Information contained in a digital certificate (cont’d.)
  - Issuer’s digital signature
  - Digital certificate’s serial number
  - Expiration date of the public key

Activity

- Use FIREFOX browser and Visit
  - www.google.com
- Click on the “three bar icon” on the left top corner
  - Click the lock icon (Privacy & Security)
  - Look for Certificates – click View Certificates
  - Find out the “certificate information” of google.com
  - For Chrome Users:
    - Click on the “More Tools → Developer Tools” Tab
- Now visit
  - http://www.findfriendz.com/
- What differences do you observe?

Managing Digital Certificates

- Technologies used for managing digital certificates
  - Certificate Authority (CA)
  - Registration Authority (RA)
  - Certificate Revocation List (CRL)
  - Certificate Repository (CR)
  - Web browser
- Certificate Authority
  - Trusted third party
  - Responsible for issuing digital certificates
  - Can be internal or external to an organization

Certificate Authority (CA)

- Duties of a CA
  - Generate, issue, an distribute public key certificates
  - Distribute CA certificates
  - Generate and publish certificate status information
  - Provide a means for subscribers to request revocation
  - Revoke public-key certificates
  - Maintain security, availability, and continuity of certificate issuance signing functions

Certificate Authority (CA)

- Subscriber requesting a digital certificate
  - Generates public and private keys
  - Sends public key to CA
  - CA may in some instances create the keys
  - CA inserts public key into certificate
  - Certificates are digitally signed with private key of issuing CA

Registration Authority (RA)

- Registration Authority
  - Subordinate entity designed to handle specific CA tasks
    - Offloading registration functions creates improved workflow for CA
- General duties of an RA
  - Receive, authenticate, and process certificate revocation requests
  - Identify and authenticate subscribers

Certificate Revocation List (CRL)

- Certificate Revocation List
  - Lists digital certificates that have been revoked
- Reasons a certificate would be revoked
  - Certificate is no longer used
  - Details of the certificate have changed, such as user’s address
  - Private key has been lost or exposed (or suspected lost or exposed)

Certificate Repository (CR)

- Certificate Repository
  - Publicly accessible centralized directory of digital certificates
  - Used to view certificate status
  - Can be managed locally as a storage area connected to the CA server
  - Can be made available through a Web browser interface

Managing Digital Certificates

- Web browser management
  - Modern Web browsers preconfigured with default list of CAs
- Advantages
  - Users can take advantage of digital certificates without need to manually load information
  - Users do not need to install a CRL manually
    - Automatic updates feature will install them automatically if feature is enabled

Types of Digital Certificates

- Different categories of digital certificates
  - Class 1 through Class 5
    - Class 1: personal digital certificates
    - Class 2: server digital certificates
    - Class 3: software publisher digital certificates
- Other uses for digital certificates
  - Provide secure communication between clients and servers by encrypting channels
  - Encrypt messages for secure Internet e-mail communication
  - Verify the identity of clients and servers on the Web
  - Verify the source and integrity of signed executable code

Activity 2

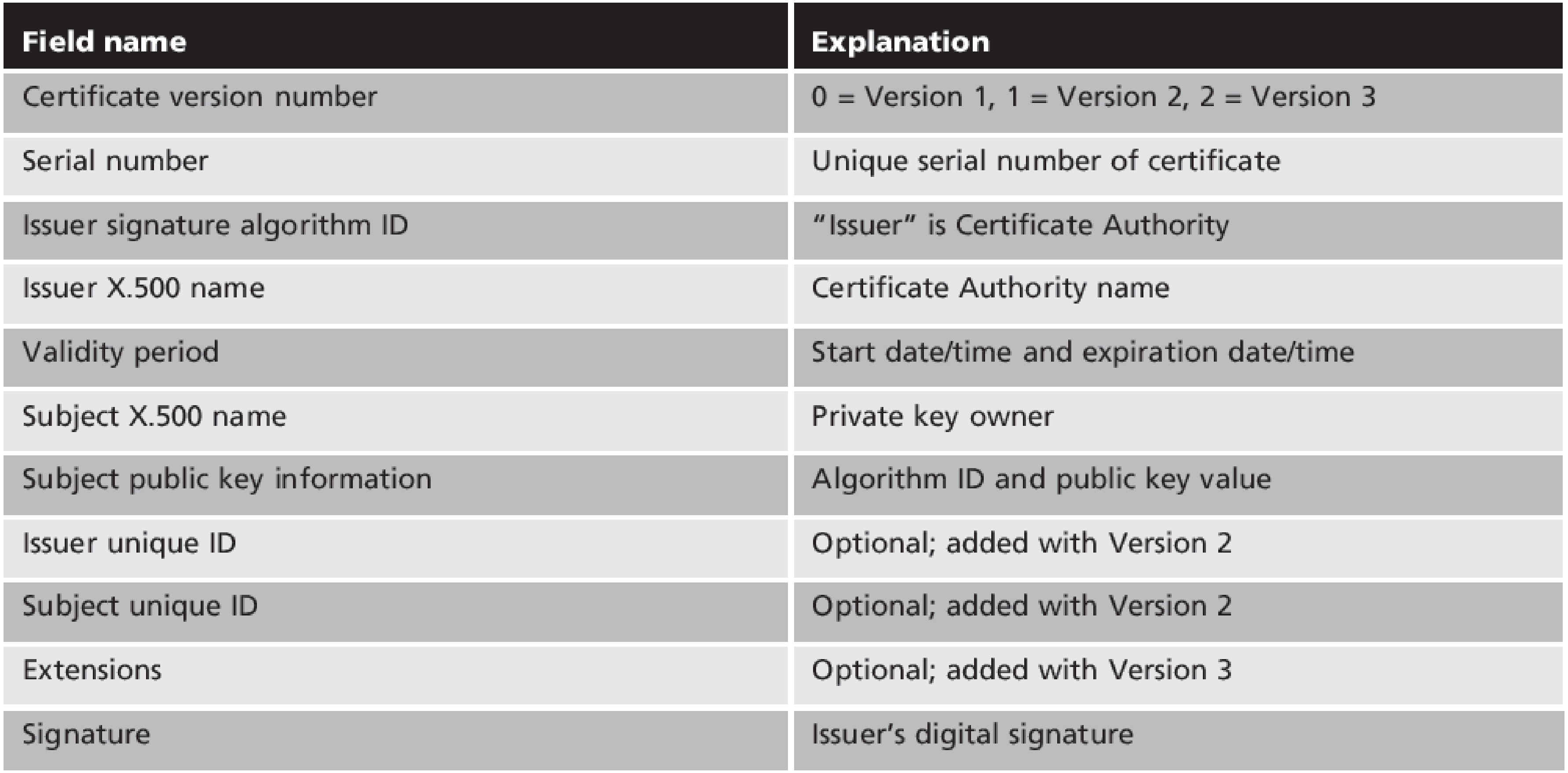
- □ Where are your web browser certificates stored?
- □ List few of them
- □ What else do you observe in the certificate store?
- □ Do you see the revocation list?

X.509 Digital Certificate Standard

- X.509 digital certificates
  - Standard for most widely accepted format for digital certificates

X.509 Digital Certificate Standard

X.509 STRUCTURE



Field name	Explanation
Certificate version number	0 = Version 1, 1 = Version 2, 2 = Version 3
Serial number	Unique serial number of certificate
Issuer signature algorithm ID	"Issuer" is Certificate Authority
Issuer X.500 name	Certificate Authority name
Validity period	Start date/time and expiration date/time
Subject X.500 name	Private key owner
Subject public key information	Algorithm ID and public key value
Issuer unique ID	Optional; added with Version 2
Subject unique ID	Optional; added with Version 2
Extensions	Optional; added with Version 3
Signature	Issuer's digital signature

Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI)

- Important management tool for the use of:
  - Digital certificates:
  - Asymmetric cryptography
- Aspects of PKI
  - Public-key cryptography standards
  - Trust models
  - Key management

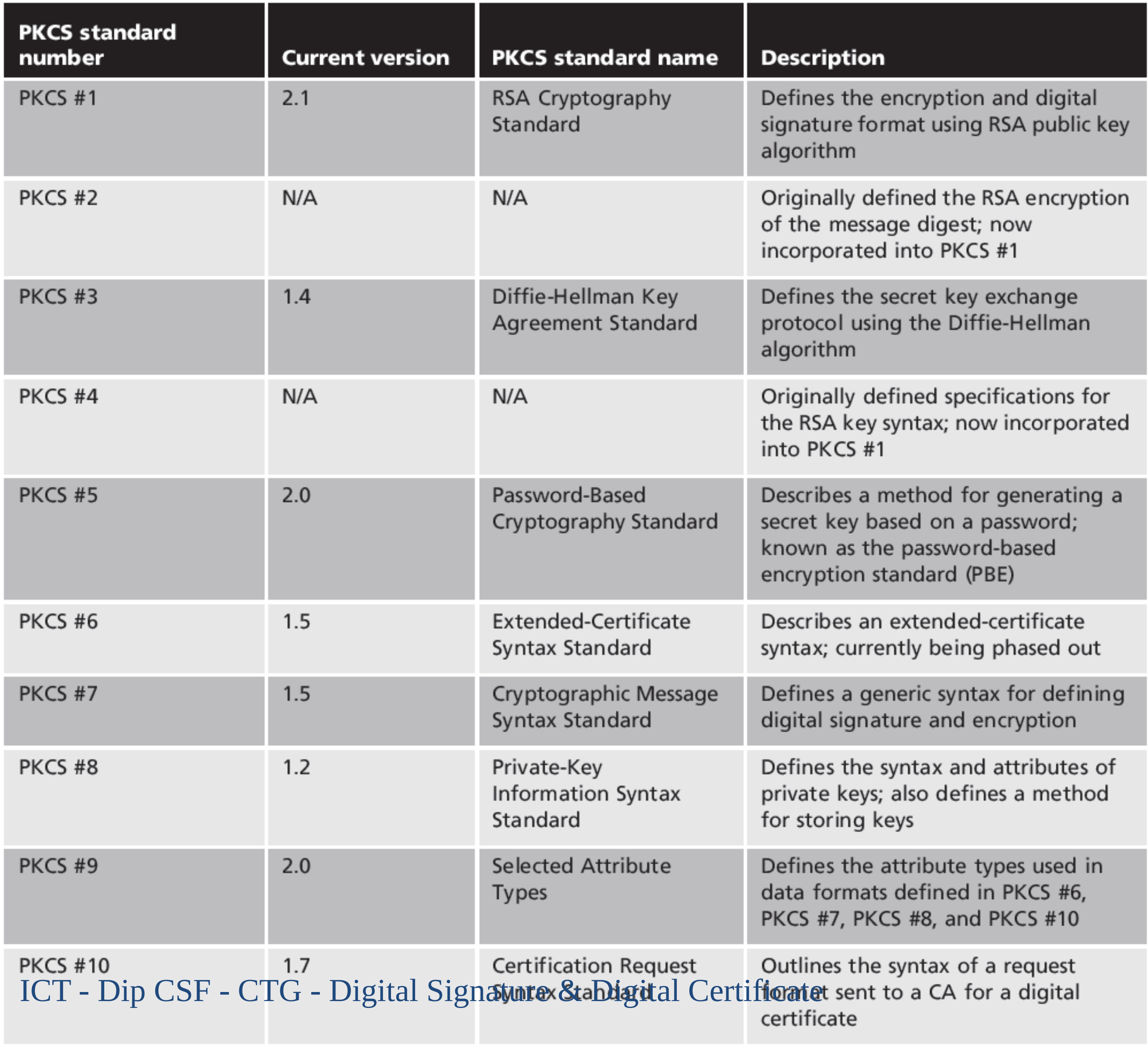
What is Public Key Infrastructure?

- Need for consistent means to manage digital certificates
- PKI: framework for all entities involved in digital certificates
- Certificate management actions facilitated by PKI
  - Create
  - Store
  - Distribute
  - Revoke

Public-Key Cryptographic Standards (PKCS)

- Numbered set of PKI standards defined by the RSA Corporation
  - Widely accepted in industry
  - Based on the RSA public-key algorithm

Public-Key Cryptographic Standards (PKCS)



PKCS standard number	Current version	PKCS standard name	Description
PKCS #1	2.1	RSA Cryptography Standard	Defines the encryption and digital signature format using RSA public key algorithm
PKCS #2	N/A	N/A	Originally defined the RSA encryption of the message digest; now incorporated into PKCS #1
PKCS #3	1.4	Diffie-Hellman Key Agreement Standard	Defines the secret key exchange protocol using the Diffie-Hellman algorithm
PKCS #4	N/A	N/A	Originally defined specifications for the RSA key syntax; now incorporated into PKCS #1
PKCS #5	2.0	Password-Based Cryptography Standard	Describes a method for generating a secret key based on a password; known as the password-based encryption standard (PBE)
PKCS #6	1.5	Extended-Certificate Syntax Standard	Describes an extended-certificate syntax; currently being phased out
PKCS #7	1.5	Cryptographic Message Syntax Standard	Defines a generic syntax for defining digital signature and encryption
PKCS #8	1.2	Private-Key Information Syntax Standard	Defines the syntax and attributes of private keys; also defines a method for storing keys
PKCS #9	2.0	Selected Attribute Types	Defines the attribute types used in data formats defined in PKCS #6, PKCS #7, PKCS #8, and PKCS #10
PKCS #10	1.7	Certification Request Syntax Standard	Outlines the syntax of a request format sent to a CA for a digital certificate

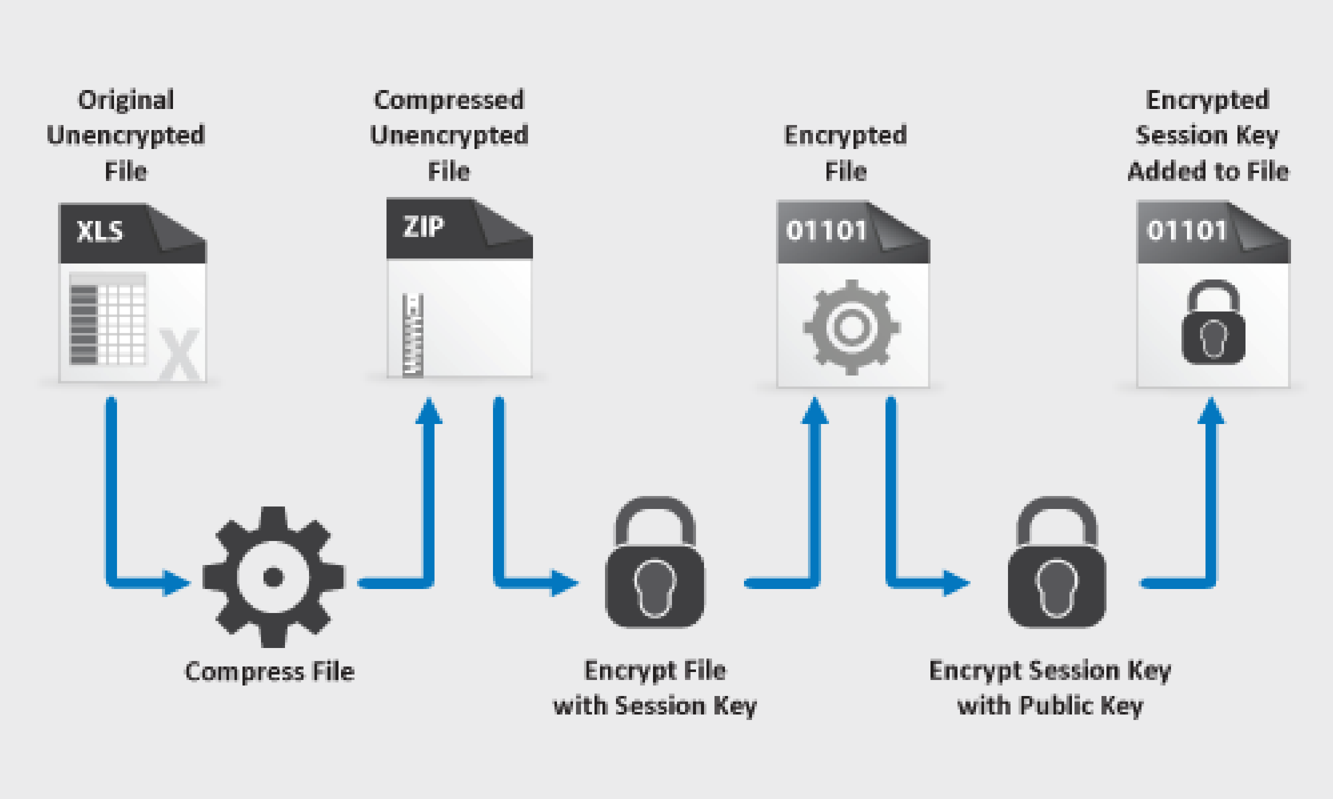
Pretty Good Privacy (PGP)

Pretty Good Privacy (PGP)

- Created by Phil Zimmermann in 1991
  - Reference: http://www.pgpi.org/doc/pgpintro/
- used for signing, encrypting, and decrypting texts, e-mails, and files.
- “OpenPGP” is now a standard (RFC 4880) since 2007
- Popular OpenPGP software
  - Mailvelope
  - Gpg4win (windows)
  - GPG Suite (Mac)

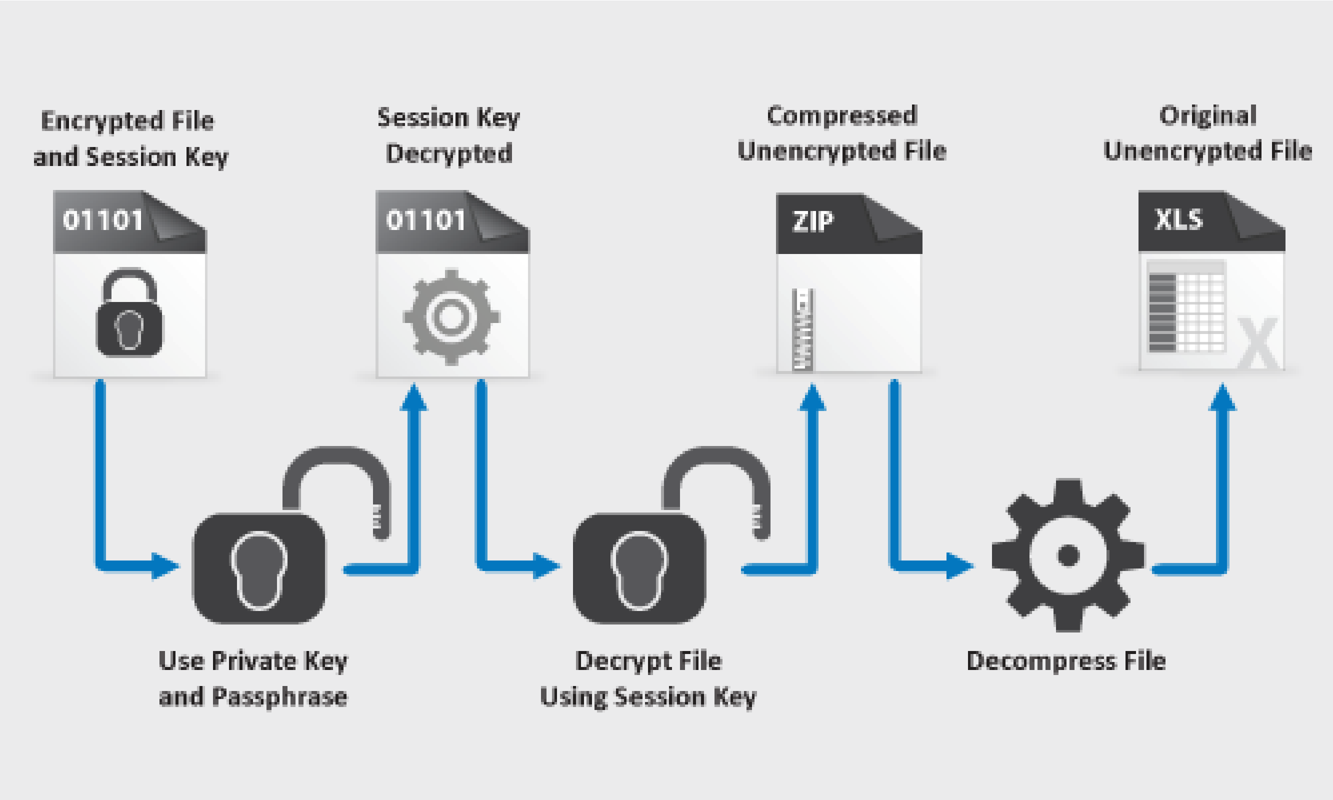
Knowledge Component

PGP Encryption


Original Unencrypted File
XLS
Compressed Unencrypted File
ZIP
Encrypted File
01101
Encrypted Session Key Added to File
01101
Compress File
Encrypt File with Session Key
Encrypt Session Key with Public Key

Source: http://www.pro2col.com/vendors/globalscape/globalscape-eft-server/openpgp-module/

PGP Decryption



Source: http://www.pro2col.com/vendors/globalscape/globalscape-eft-server/openpgp-module/

Mailvelope

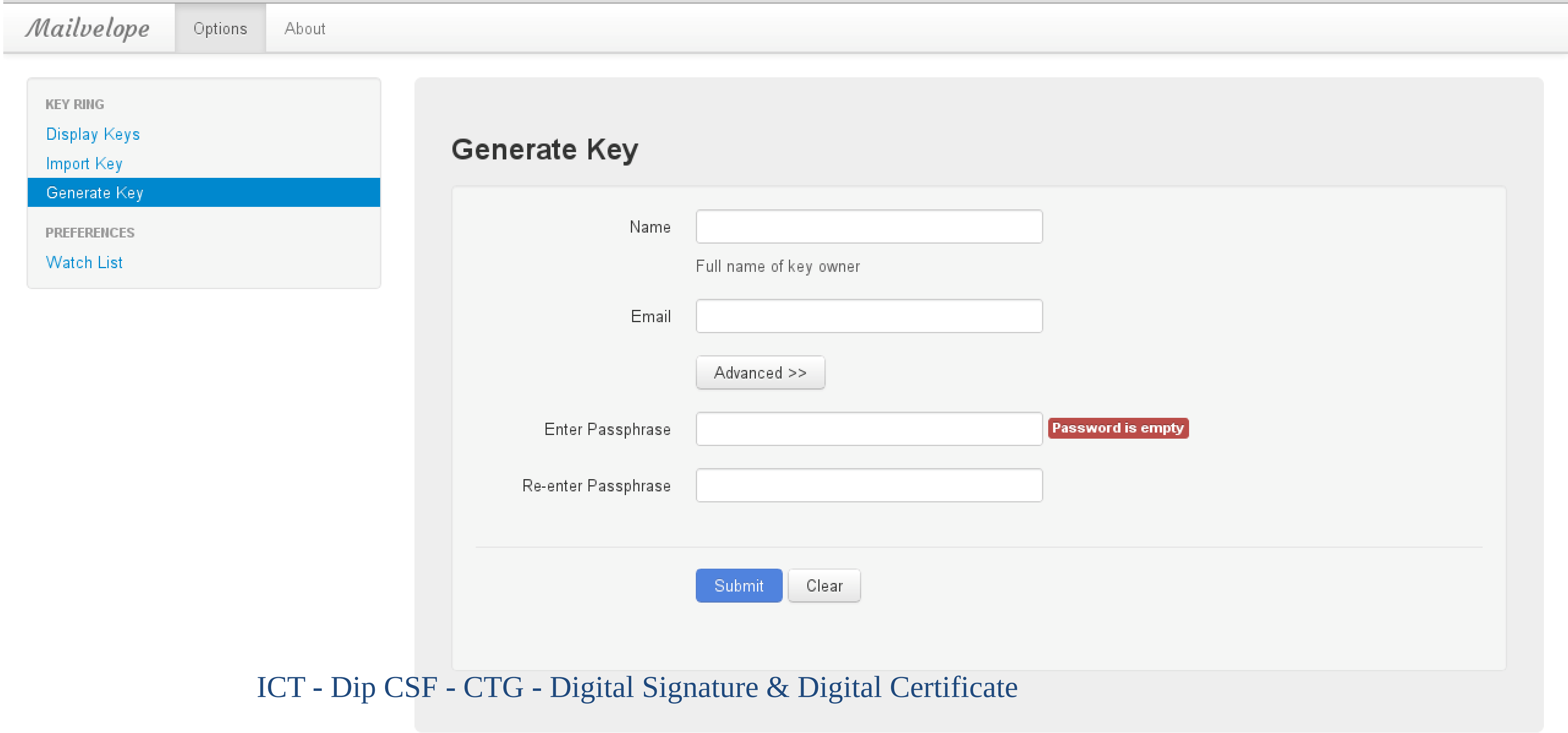
- OpenPGP encryption for webmail
  - Gmail
  - Yahoo! Mail
  - Outlook.com
- URL
  - https://www.mailvelope.com/
- Documentation
  - https://www.mailvelope.com/help

Install Mailvelope Extension

- It is a plugin for browser
  - https://www.mailvelope.com/en/
- Restart Browser

Generate Key

- Mailvelope Icon next to the address bar
- Click on Mailvelope Icon → Options → Generate Key



Generate Key

Name

Full name of key owner

Email

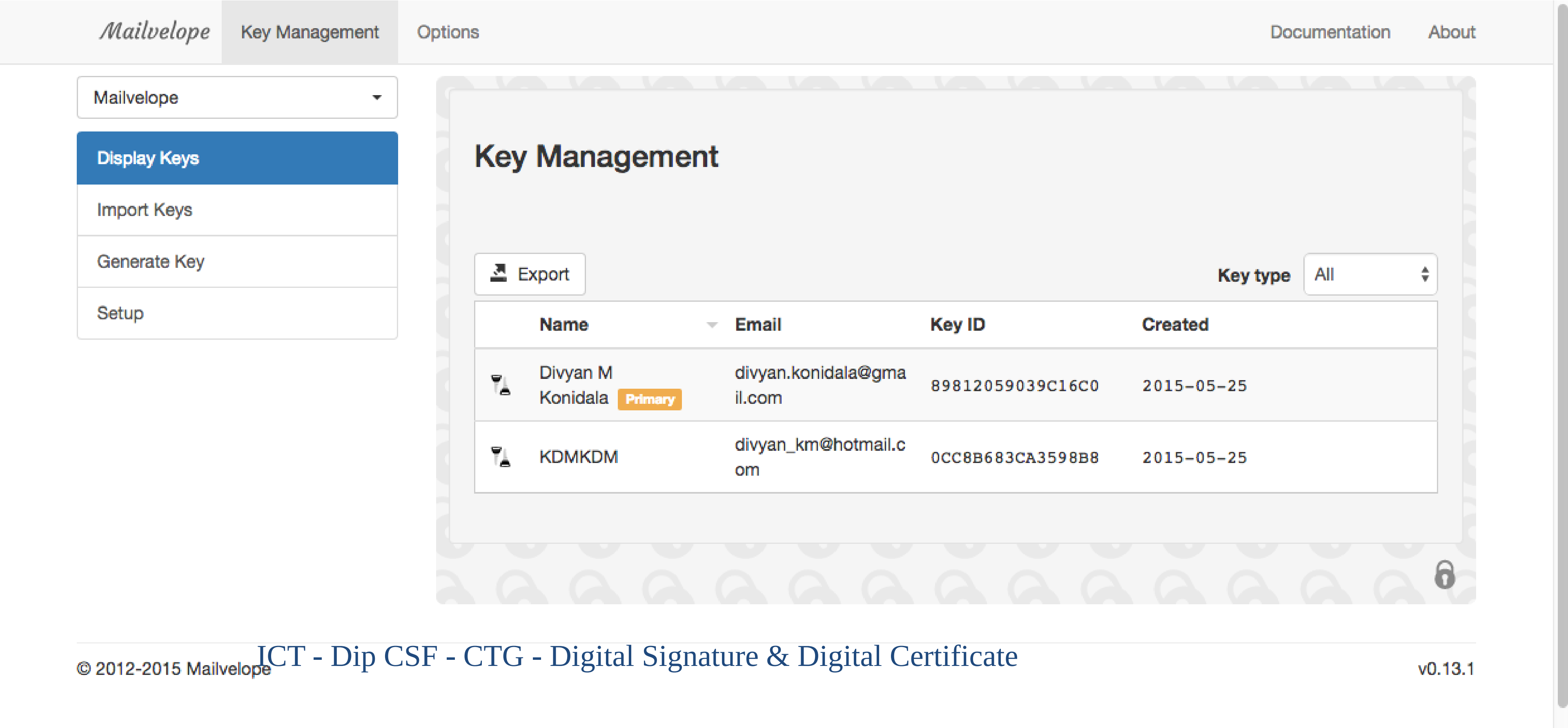
Enter Passphrase

Password is empty

Re-enter Passphrase

Display Keys

- Mouse over the key and click on "i" button that appears. What is your public and private key?

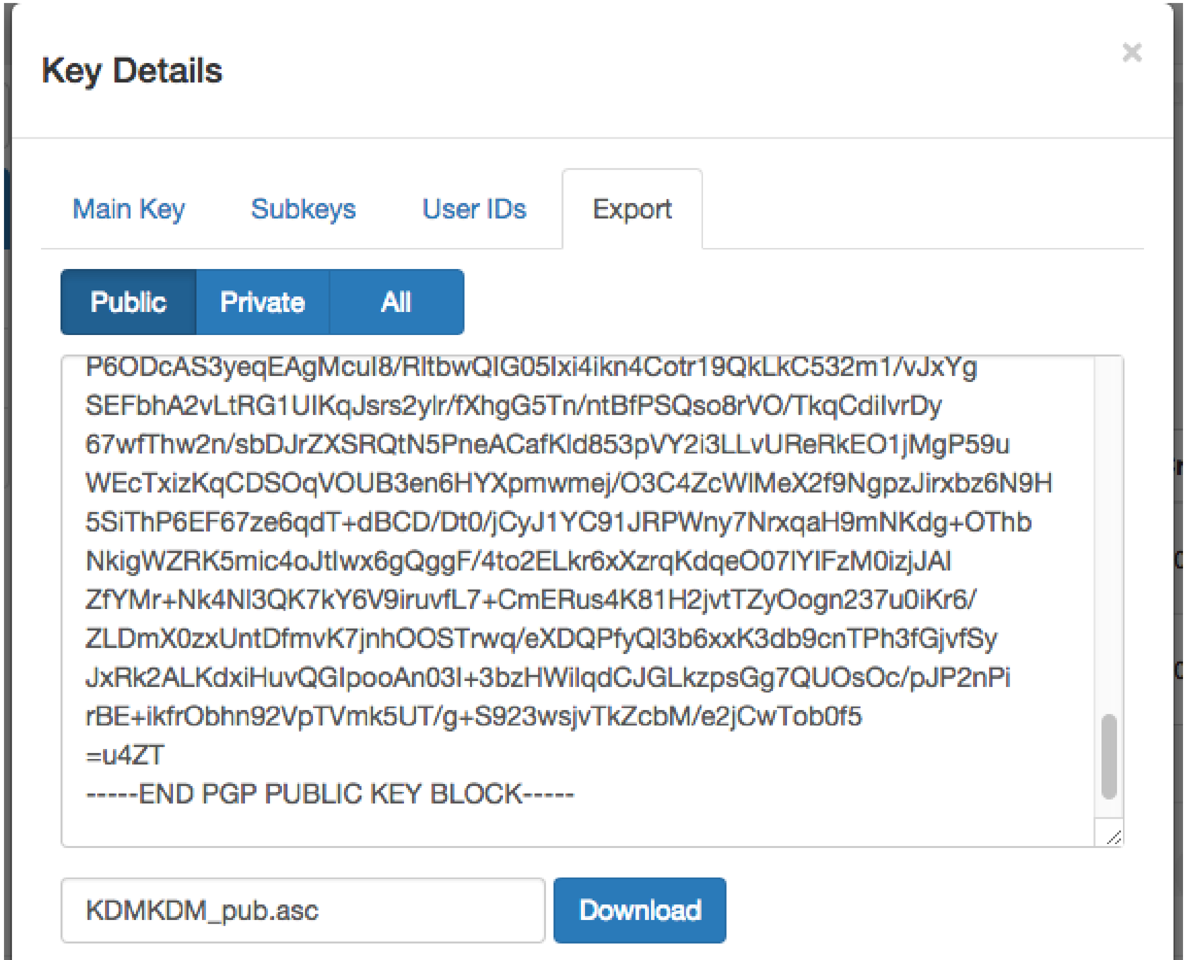


Key Management

Name	Email	Key ID	Created
Divyan M Konidala Primary	divyan.konidala@gmail.com	89812059039C16C0	2015-05-25
KDMKDM	divyan_km@hotmail.com	0CC8B683CA3598B8	2015-05-25

© 2012-2015 Mailvelope

Export Public Key



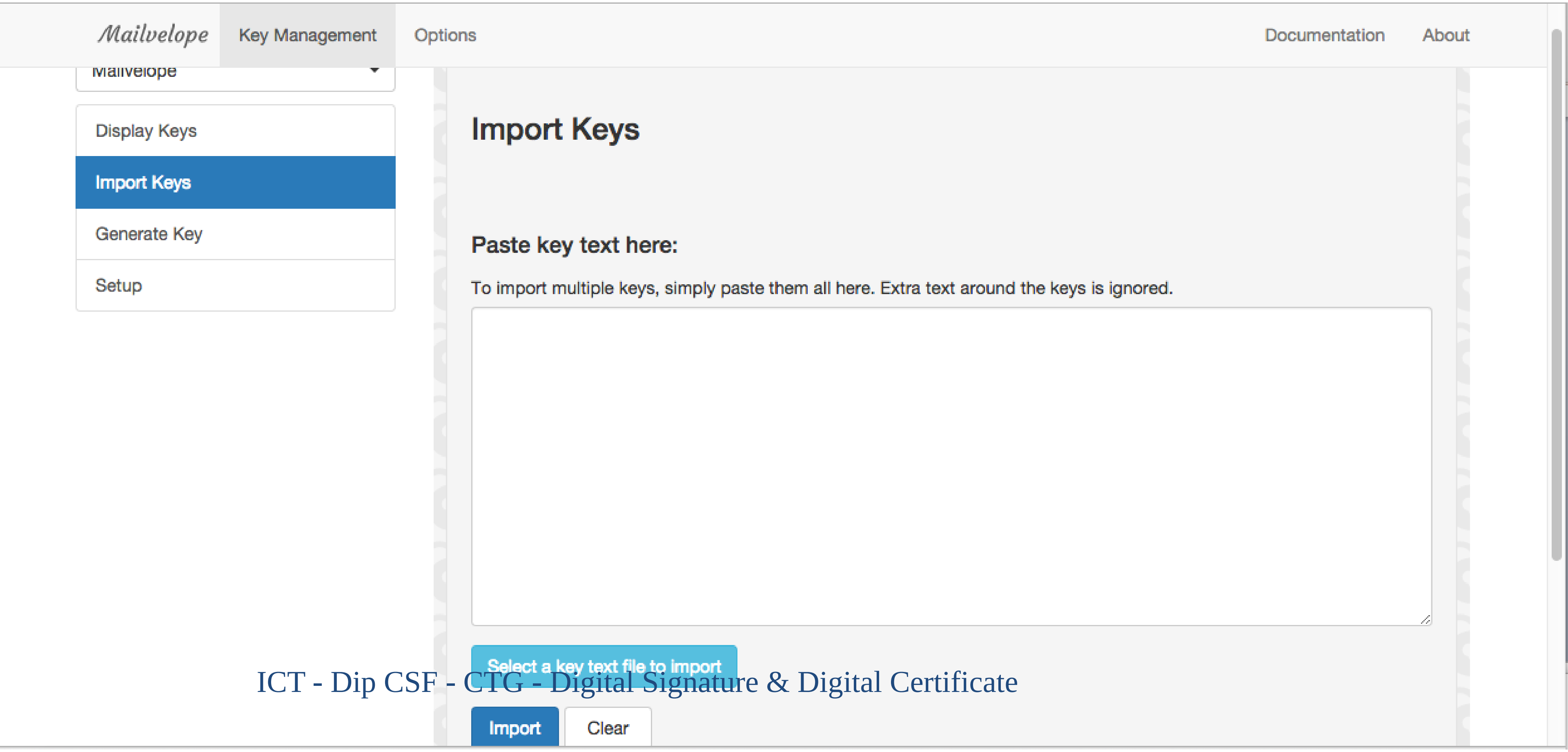
P6ODcAS3yeqEAgMcuI8/RltbwQIG05Ixi4ikn4Cotr19QkLkC532m1/vJxYg
SEFbhA2vLtRG1UIKqJsrs2ylr/fXhgG5Tn/ntBfPSQso8rVO/TkqCdilvrDy
67wfThw2n/sbDJrZXSRQtN5PneACafKld853pVY2i3LLvUReRkEO1jMgP59u
WEcTxizKqCDSOqVOUB3en6HYXpmwmej/O3C4ZcWIMeX2f9NgpzJirxbz6N9H
5SiThP6EF67ze6qdT+dBCD/Dt0/jCyJ1YC91JRPWny7NrxqaH9mNKdg+OThb
NkigWZRK5mic4oJtlwx6gQggF/4to2ELkr6xXzrqKdqeO07IYIFzM0izjJAI
ZfYMr+Nk4NI3QK7kY6V9iruvfL7+CmERus4K81H2jvtTZyOogn237u0iKr6/
ZLDmX0zxUntDfmvK7jnhOOSTrwq/eXDQPfyQI3b6xxK3db9cnTPh3fGjvfSy
JxRk2ALKdxiHuvQGIpooAn03I+3bzHWilqdCJGLkzpsGg7QUOsOc/pJP2nPi
rBE+ikfrObhn92VpTVmk5UT/g+S923wsjvTkZcbM/e2jCwTob0f5
=u4ZT
-----END PGP PUBLIC KEY BLOCK-----

KDMKDM_pub.asc

- □ Download your public key
- □ Email your public key to your friend

Import Keys

- □ Import your friend’s public key



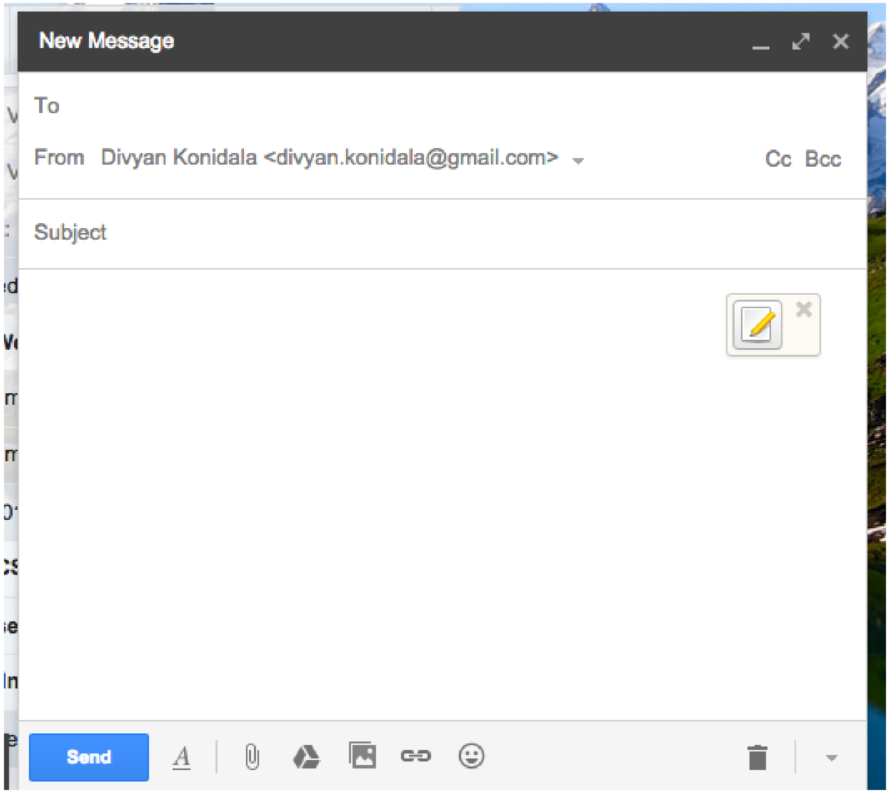
Import Keys

Paste key text here:

To import multiple keys, simply paste them all here. Extra text around the keys is ignored.

Compose Email

- □ Click on the pen-notepad button (text encryption)



New Message

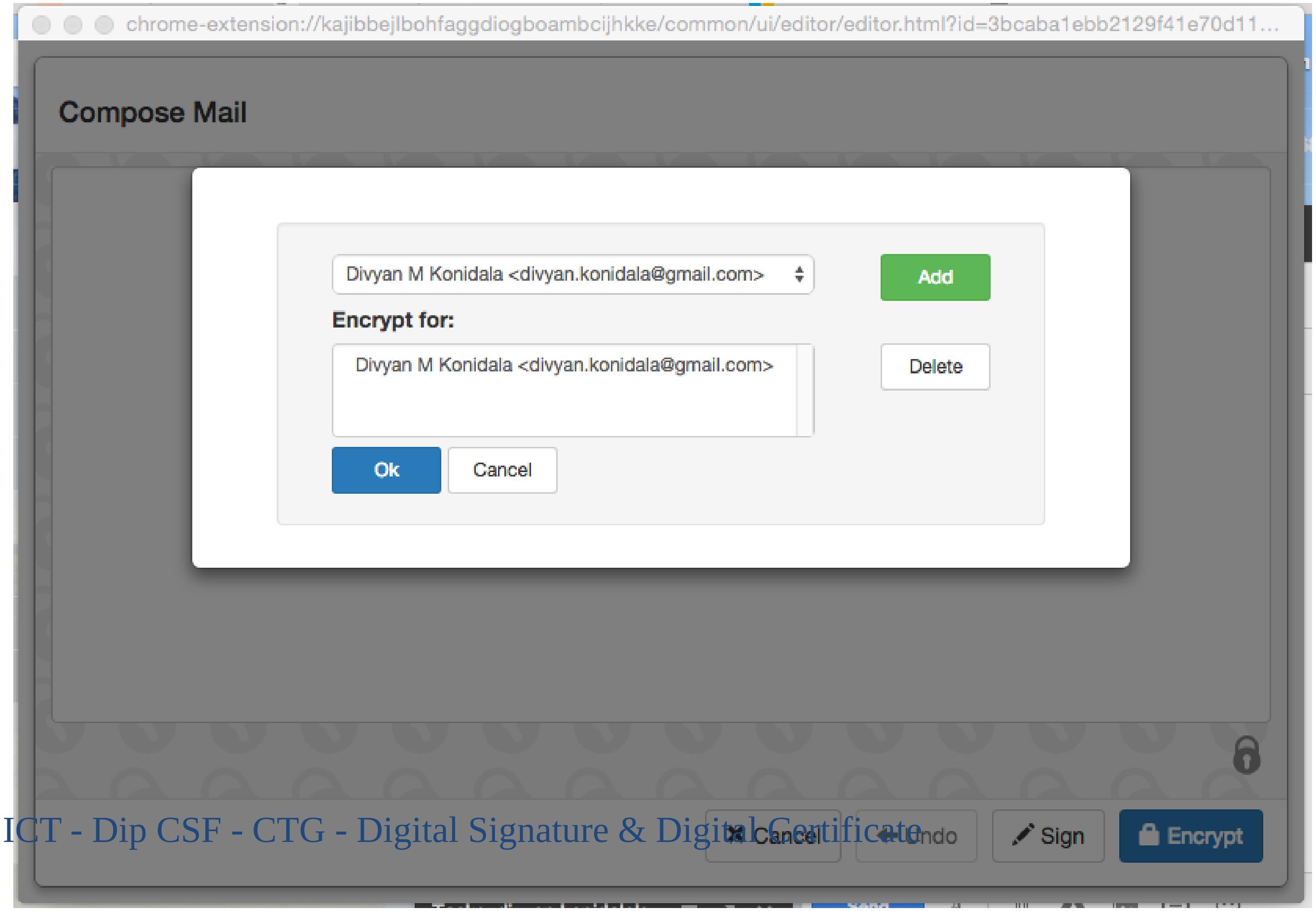
To

From Divyan Konidala <divyan.konidala@gmail.com>

Subject

Compose Email - Encrypt

- □ Select your friend’s public key
- □ Click “OK” → “Transfer” → “Send”



chrome-extension://kajibbejlbohfaggdiogboambcijhkke/common/ui/editor/editor.html?id=3bcaba1ebb2129f41e70d11…

Compose Mail

Divyan M Konidala <divyan.konidala@gmail.com>

Encrypt for:

Divyan M Konidala <divyan.konidala@gmail.com>

Explore the following

- How do you decrypt?
- How do you sign a message?

Skill – Using GPG4WIN (optional)

- Gpg4win
  - GNU Privacy Guard for Windows
  - a secure solution
  - for file and email encryption. Gpg4win is Free Software and can be installed with just a few mouse clicks.
- URL: http://www.gpg4win.org/index.html
- Download: http://www.gpg4win.org/download.html
  - Gpg4win 2.3.3
- Documentation
  - Contents: Part I – Chapters 6 ~ 13
  - http://www.gpg4win.org/doc/en/gpg4win-compendium.html

Summary

Week 6.1

You learnt about

- Digital certificate
  - Defining digital certificate
  - Managing digital certificates
    - CA, RA, CRL, CR
  - Types of digital certificates
  - X.509 digital certificate standard
- Public-Key infrastructure (PKI)
- Pretty Good Privacy (PGP)