Microsoft Office Outlook PGP Add-in

Group 37

Instituto Superior Tecnico

December 15, 2013

Overview

1. Introduction
2. Implementation
3. Conclusion

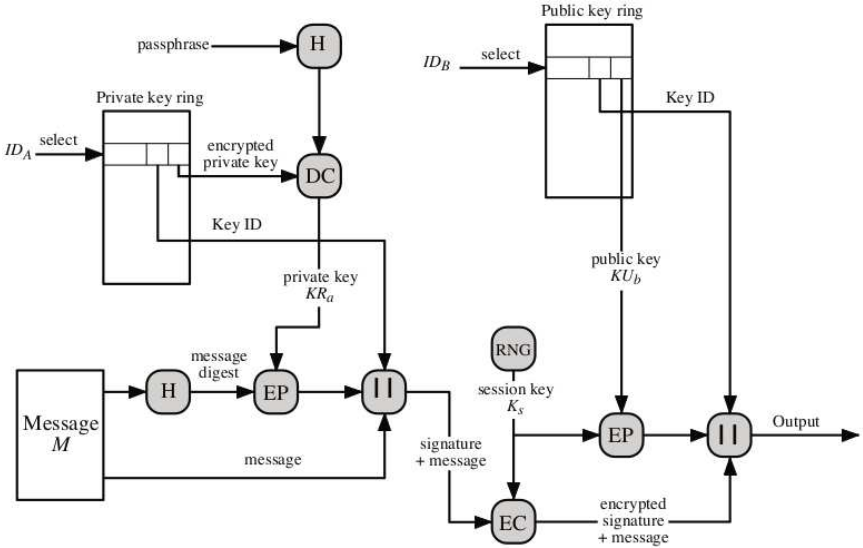
OpenPGP

- PGP, GnuPG, OpenPGP
- Used for:
  - Digital Signature (SHA1,MD5,SHA256)
  - Message Encryption (AES,CAST; RSA)
  - Compression (ZIP)
  - Compatibility (Radix-64)
- RFC 4880
- Interoperability
- Legal issues

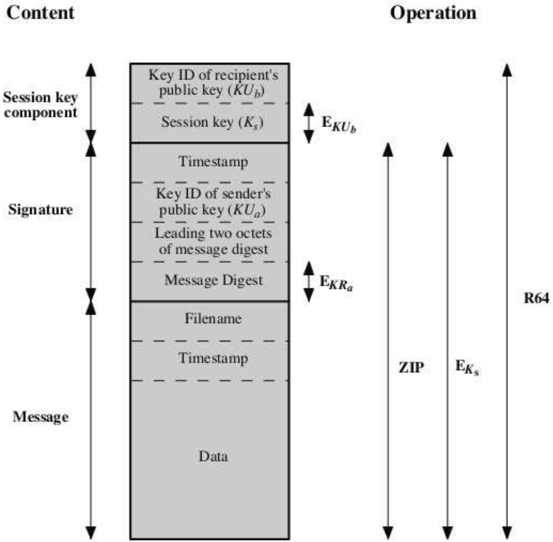
How it works

1. 4 key types: passphrase, session-key, private key, public key
2. Public and private key rings
3. Passphrase encrypts private key ring
4. Every user can have a public-private key pair

How it works


passphrase
H
Public key ring
ID_B
select
Private key ring
Key ID
ID_A
select
encrypted private key
DC
Key ID
private key KR_a
public key KU_b
RNG
message digest
Message M
H
EP
| |
session key K_s
message
signature + message
EP
| |
Output
EC
encrypted signature + message

How it works



Content

Operation

Session key component

Key ID of recipient's public key (KU_b)

Session key (K_s)

E_{KU_b}

Signature

Timestamp

Key ID of sender's public key (KU_a)

Leading two octets of message digest

Message Digest

E_{KR_a}

Message

Filename

Timestamp

Data

ZIP

E_{K_s}

R64

Implementation

Initial Design

Microsoft CryptoAPI + Bouncy Castle API

Current Implementation

- Didisoft's .NET API
- Default choices:
  - Key Size: 2048 bits [1]
  - Asymmetric Algorithm: RSA
  - Symmetric Cipher: AES-128/CAST5
  - Hash function: SHA1, MD5, SHA256
  - Compression: ZIP

Implementation

Table

Theorem

Verbatim

Lessons learned

- Poorly documented APIs are *not good*
- Existing Didisoft limitations [2]

Future work

- PGP/MIME support (attachments)
- ECDSA and ECDH?
- Advanced users configuration
- Keccak (SHA3) *vs.* MD5 or SHA1 (vulnerable [3])
- More configurable

References

Elaine Barker, Allen Roginsky (2011)
Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths
NIST Special Publication 800-131A

www.didisoft.com
OpenPGP Email messages
http://www.didisoft.com/net-openpgp/examples/openpgp-email-messages/

Marc Stevens
Framework for MD5 & SHA-1 Differential Path Construction and Chosen-Prefix Collisions for MD5
https://code.google.com/p/hashclash/

Demo