Microsoft Office Outlook PGP Add-in

Group 37

Instituto Superior Técnico

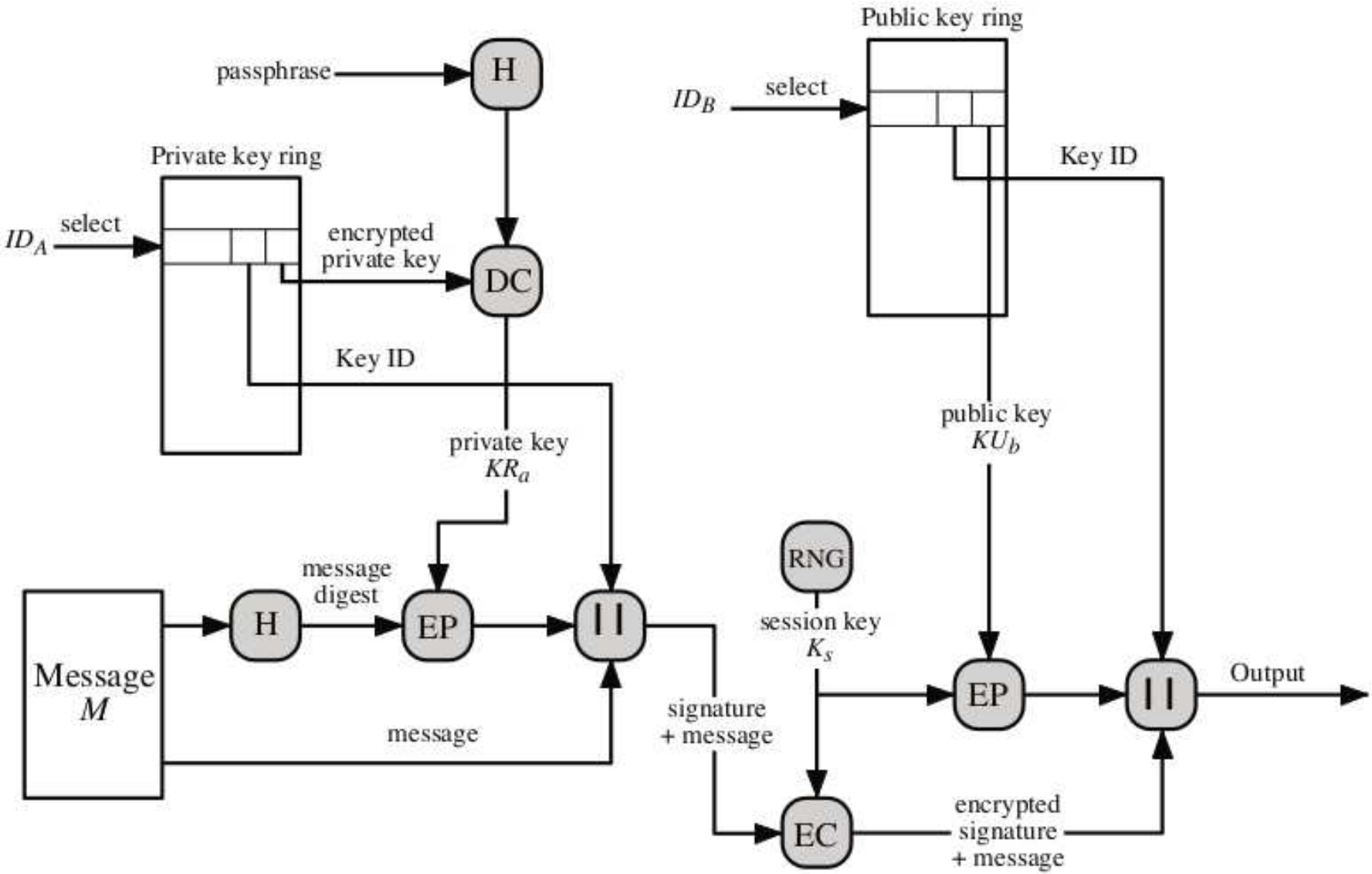
December 19, 2013

Overview

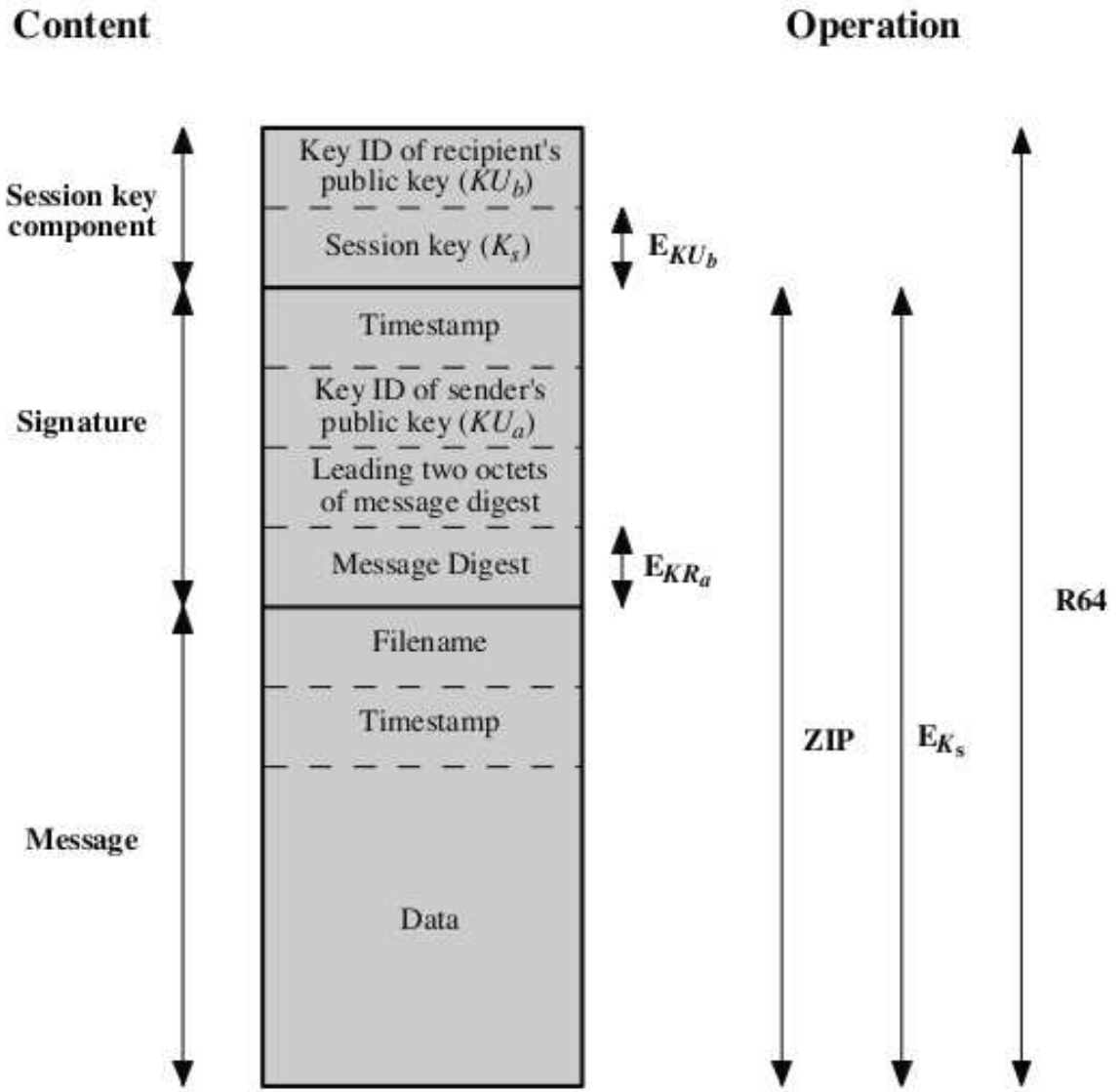
OpenPGP

- PGP, GnuPG, OpenPGP
- Services offered:
  - Digital Signature
  - Message Encryption
  - Compression
  - Compatibility
- Interoperability
- Legal issues

How it works


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

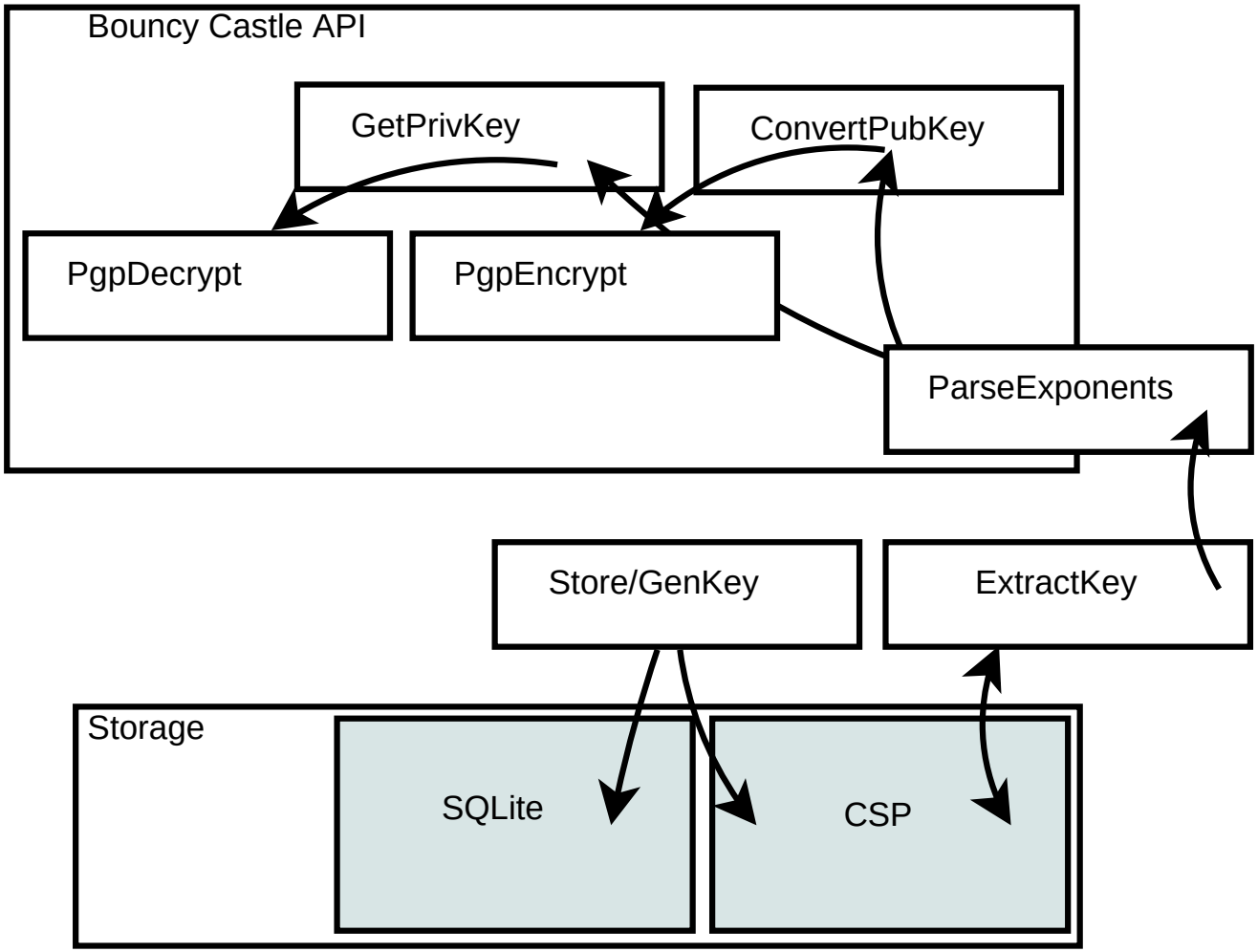
How it works


Content
Operation
Session key component
Signature
Message
Key ID of recipient's public key (KU_b)
Session key (K_s)
Timestamp
Key ID of sender's public key (KU_a)
Leading two octets of message digest
Message Digest
Filename
Timestamp
Data
E_{KU_b}
E_{KR_a}
ZIP
E_{K_s}
R64

Implementation - 1st Iteration: Bouncy Castle API

- Microsoft CryptoServiceProvider
- SQLite for key/contacts information
- Bouncy Castle Open Source Cryptographic functions

Design


Bouncy Castle API
GetPrivKey
ConvertPubKey
PgpDecrypt
PgpEncrypt
ParseExponents
Store/GenKey
ExtractKey
Storage
SQLite
CSP

Implementation - 2nd Iteration: Didisoft API

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

Implementation - RSA vs. DSA2/ElGamal

RSA

- Integer Factorisation
- Default in GPG [4]
- More wide-spread
- Faster signature verification
- Longer signatures

DSA2 with ElGamal

- Discrete Logarithm Problem
- Smaller signatures
- Slightly faster signature generation
- Shorter key length

We need something simpler

- public key
- private key
- certificates
- key rings
- does your mom understand it?

Lessons learned

- Poorly documented APIs are *not good*
- Didisoft API limited to inline encryption [2]
- Implementing OpenPGP is *hard*

Future work?

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

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/

Nathan Willis(June 17, 2009)

Dealing with weakness in SHA-1

http://lwn.net/Articles/337745/

Demo