PKWARE

SecureZIP for Linux on System z

2012 VM Workshop

Robb Ervin • Director of Solution Engineering

A Revolution in Managing, Moving, Storing and Securing Data Across the Extended Enterprise

PKWARE®

A Revolution in Managing, Moving, Storing and Securing Data Across the Extended Enterprise.

This session explores how data can move securely and efficiently from Linux on System z to the extended enterprise. We will discuss how Linux for System z can work cooperatively with AIX, Linux for x86 and Windows Server on the z/BX as well as stand-alone hardware alongside of z/OS, IBM i, Solaris and HP-UX. Uses cases covered include protecting data with symmetric and asymmetric encryption, as well as digital signing and authentication on Linux for System z, including passphrase, X.509 digital certificates and PGP keys.

Data Encryption

Symmetric Encryption = Password

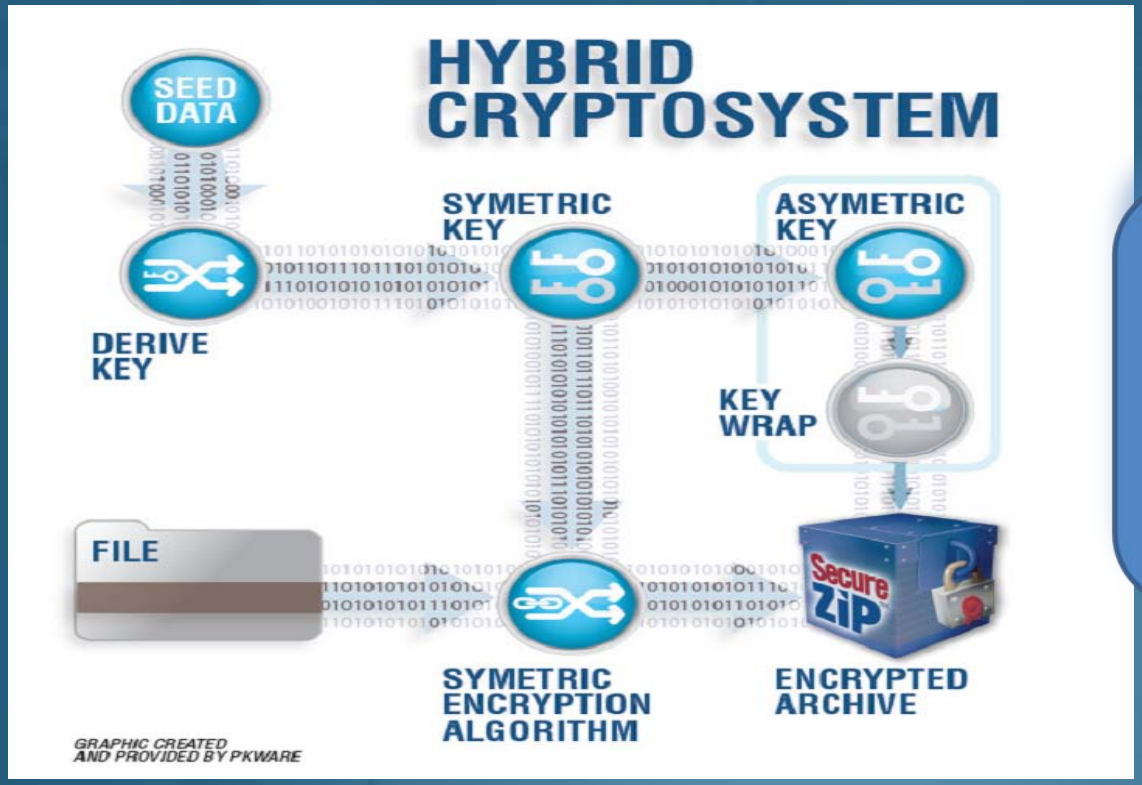
- Secured data by specifying a password
- Share that same password with the receiving user to use when decrypting the secured file
- Shorter passwords are subject to compromise by simple brute force attached
- The longer & more complex password, the better
- The stronger the algorithm (AES-128 or 256-bit) the better

Data Encryption

Asymmetric Encryption = Digital Certificates

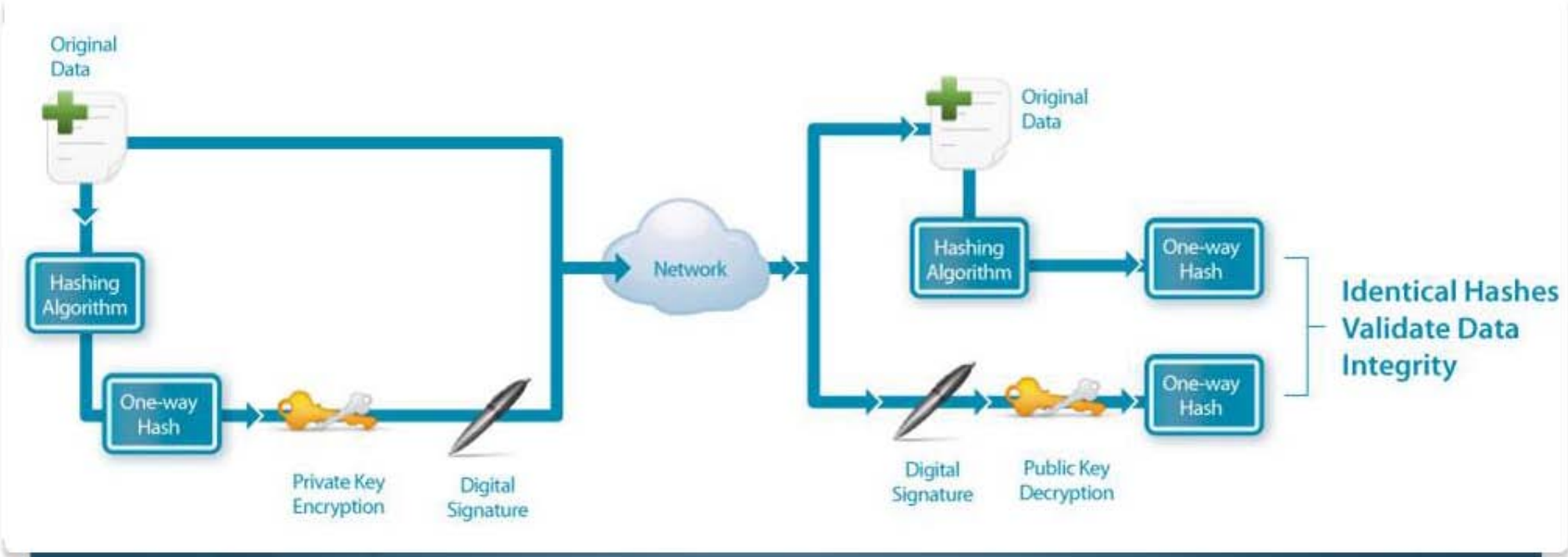
- Obtained from a Certification Authority (i.e. VeriSign, Comodo) or self-generated (i.e. PGP Keys)
- Consists of a public/private key pair
- Share your public key with other users to encrypt data that will be sent to you
- ***Never*** share your private key!
- Use your private key to decrypt the data that was encrypted with your public key

Data Encryption



SecureZIP is implemented as a hybrid cryptosystem.

Digital Signing and Authentication



Why is it important?

Digital signatures such as those supported today by SecureZIP provide integrity and identity verification … they provide “trust”

- Through a digital signature, we can detect if a single bit in a file has been altered since it was signed
- Signing with a digital certificate provides assurances that the file was signed by right person
  - A file signed by an unexpected person, or a file having a digital signature that cannot be verified signals the information may not be as it seems and should not be trusted (even though the signature may validate)

z196 and z114 Interoperability with zBX

PKWARE Product Portfolio

PKZIP®	SecureZIP®
Windows Desktop	Windows Desktop
Windows Server	Windows Server
HP-UX	HP-UX
Solaris	Solaris
Linux - x86	Linux - x86
● Linux - System z	● Linux - System z
AIX	AIX
IBM i	IBM i
z/OS	z/OS

PKWARE Linux on System z

- Traditional command line interface
- Java Software Developers Kit (SDK)

Use Case

Major Pharmaceutical

- Primary order & distribution systems are legacy z/OS, generating complex customer-specific lists of medications & details
- Files must be compressed before transmission to customers to meet SLA/SLO
- High volume each month, driving z/OS peaks, increasing environment costs
- Transfer lists from z/OS to Linux on System z, reducing costs & improving service delivery

Use Case

National Brokerage Firm

- Integrated SecureZIP for Linux [x86] into several workflows managing sensitive data (SSN's, CCN's, brokerage account #'s, etc.)
- Determined that consolidation of Linux x86 servers to Linux on System z improved system up-time and availability, reduced TCO over time
- While some application components required replacement, SecureZIP for Linux on System z supported seamless migration of data protection

SecureZIP v14

V14 Supports Two Security Formats

.ZIP

x.509
Passphrase
OpenPGP Keys (RSA Only)

OPENPGP

Passphrase
OpenPGP Keys

Contingency Key can include X.509 or OpenPGP

SecureZIP v14

OpenPGP Format Support based on RFC4880

Binary
ASCII Armor
PGP-Zip

OpenPGP Key Support

RSA (Signature and Encryption)
DSA (Signature only)
ElGamal (Encryption only)

```
java -jar PKKeyM.jar generate -outPublicPGP
/home/robb_e/.pgp/pubring.pkr –outSecretPGP
/home/robb_e/.pgp/secring.skr -outPass pktestr2012 -userid
"PK Encrypt<PKSecurity@pkware.com>"

PKWARE(R) Key Maker(TM) Version 1.00.0004
Portions copyright(c) 1989-2012 PKWARE, Inc.  All Rights Reserved.

Generating 2048-bit RSA Key Pair
Generating OpenPGP Key

Created OpenPGP key
   User ID: PK Encrypt<PKSecurity@pkware.com>
   Key ID: CEE37B9FD9FB979A
   Key Type: RSA
   Key Size: 2048
   Created: Wed Jun 27 21:37:43 EDT 2012
   Expires: Never
   Key Validity: Unknown
   Thumbprint: 9F8A 1275 2E19 F711 BF2C 1B1D CEE3 7B9F D9FB 979A
Updating secret keyring: /home/robb_e/.pgp/secring.skr
Updating public keyring: /home/robb_e/.pgp/pubring.pkr
Finished
```

```
java -jar PKKeyM.jar generate -outPublicPGP
/home/robb_e/.pgp/pubring.pkr –outSecretPGP
/home/robb_e/.pgp/secring.skr -outPass pktests2012 -userid
"PK Signing<PKSupport@pkware.com>"

PKWARE(R) Key Maker(TM) Version 1.00.0004
Portions copyright(c) 1989-2012 PKWARE, Inc.  All Rights Reserved.

Generating 2048-bit RSA Key Pair
Generating OpenPGP Key

Created OpenPGP key
   User ID: PK Signing<PKSupport@pkware.com>
   Key ID: BFA08A84F73B3C00
   Key Type: RSA
   Key Size: 2048
   Created: Wed Jun 27 21:39:01 EDT 2012
   Expires: Never
   Key Validity: Unknown
   Thumbprint: 7B4A E8CC 544E DCDE 06AB C83F BFA0 8A84 F73B 3C00
Updating secret keyring: /home/robb_e/.pgp/secring.skr
Updating public keyring: /home/robb_e/.pgp/pubring.pkr
Finished
```

```
pkzipc -add -archivetype=pgp -cryptalg=aes,256
-passphrase=2012vmworkshop -recipient="PK Encrypt" -sign=all
-certificate="PK Signing" -keypassphrase=pktests2012
SecuredandSigned.pgp *.txt


SecureZIP(R) Server  Version 14 for Linux s390 Registered Version
Portions copyright (C) 1989-2011 PKWARE, Inc.  All Rights Reserved.
Reg. U.S. Pat. and Tm. Off.  Patent No. 5,051,745  7,793,099  7,844,579
7,890,465  7,895,434;  Other patents pending

 Using default compression method

Creating .PGP: SecuredandSigned.pgp

  Adding File: serverfile.txt Storing      ( 0.0%), done.
```

pkzipc –listcertificates

```
SecureZIP(R) Server  Version 14 for Linux s390 Registered Version
Portions copyright (C) 1989-2011 PKWARE, Inc.  All Rights Reserved.
Reg. U.S. Pat. and Tm. Off.  Patent No. 5,051,745  7,793,099  7,844,579
7,890,465  7,895,434;  Other patents pending

Certificates available on this system are:

                          PK Encrypt: (OpenPGP)
                          PK Signing: (OpenPGP)
      PKWARE PartnerLink TEST Contingency Certificate: Valid
      PKWARE PartnerLink TEST Signing Certificate: Valid
                          Robb Ervin: (OpenPGP)
```

```
pkzipc -add -cryptalg=aes,256 -passphrase=2012vmworkshop
-recipient="PK Encrypt" -certificate="PKWARE PartnerLink TEST
Signing Certificate" -keypassphrse=pltests -sign=all
SecuredandSigned.zip *.txt


SecureZIP(R) Server  Version 14 for Linux s390 Registered Version
Portions copyright (C) 1989-2011 PKWARE, Inc.  All Rights Reserved.
Reg. U.S. Pat. and Tm. Off.  Patent No. 5,051,745  7,793,099  7,844,579
7,890,465  7,895,434;  Other patents pending

 Strongly encrypting files with recipients or a passphrase using AES (256-bit)
 Using UTF-8 file names and comments
 Using default compression method

Creating .ZIP: SecuredandSigned.zip

  Adding File: serverfile.txt Deflating    (83.6%), Encrypting, done.

Central Directory is signed by: PKWARE PartnerLink TEST Signing Certificate
```

```
pkzipc -extract -keypass=pktestr2012 SecuredandSigned.pgp


SecureZIP(R) Server  Version 14 for Linux s390 Registered Version
Portions copyright (C) 1989-2011 PKWARE, Inc.  All Rights Reserved.
Reg. U.S. Pat. and Tm. Off.  Patent No. 5,051,745  7,793,099  7,844,579
7,890,465  7,895,434;  Other patents pending

Extracting files from .PGP: /home/robb_e/SecuredandSigned.pgp

    Unstoring: serverfile.txt  OK

File is signed by: PK Signing
```

For More Information Or To Buy PKWARE Solutions Please Contact

Len Santalucia, CTO & Business Development Manager
One Penn Plaza – Suite 2010
New York, NY 10119
212-799-9375
lsantalucia@vicominfinity.com

About Vicom Infinity

- Account Presence Since Late 1990's
- IBM Premier Business Partner
- Reseller of IBM Hardware, Software, and Maintenance
- Vendor Source for the Last 4 Generations of Mainframes/IBM Storage
- Professional and IT Architectural Services
- Vicom Family of Companies Also Offer Leasing & Financing, Computer Services, and IT Staffing & IT Project Management

VICOM Infinity