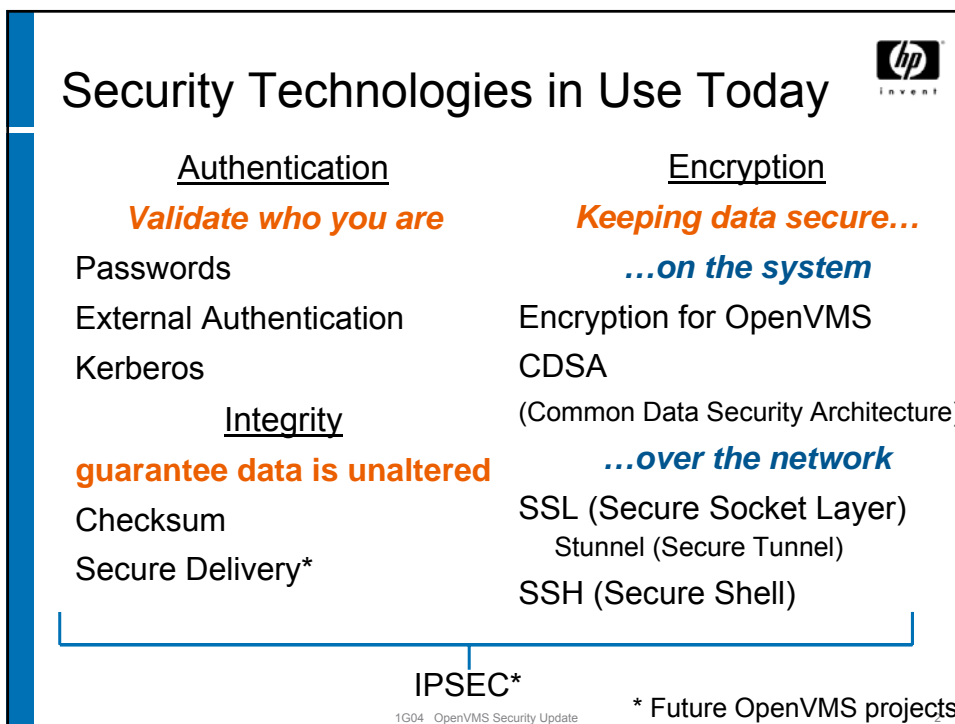



hp invent

# OpenVMS Security Update

Helmut Ammer  
CCCSC  
1G04



hp invent

## Security Technologies in Use Today

<p><u>Authentication</u></p> <p><b>Validate who you are</b></p> <p>Passwords</p> <p>External Authentication</p> <p>Kerberos</p>	<p><u>Encryption</u></p> <p><b>Keeping data secure...</b></p> <p><i>...on the system</i></p> <p>Encryption for OpenVMS</p> <p>CDSA (Common Data Security Architecture)</p>
<p><u>Integrity</u></p> <p><b>guarantee data is unaltered</b></p> <p>Checksum</p> <p>Secure Delivery*</p>	<p><i>...over the network</i></p> <p>SSL (Secure Socket Layer)</p> <p>Stunnel (Secure Tunnel)</p> <p>SSH (Secure Shell)</p>

IPSEC\*

1G04 OpenVMS Security Update

\* Future OpenVMS projects



## Agenda

- Security Roadmap
- SSL update
- External Authentication
- Kerberos Update
- Secure Delivery
- AES Encryption

1G04 OpenVMS Security Update

3



## OpenVMS Security Roadmap

2005                      2006                      2007                      2008                      2009

OpenVMS V8.2

- ACME Login EAK wt LDAP
- Kerberos 1.2
- OpenSSL 1.2
- CDSA (Secure Delivery SDK)
- Buffer Overflow Protection (Integrity Servers only)

Open Source Security Tools

- Stunnel (secure tunnel)
- GnuPG V1.2.4

OpenVMS V8.3

- Production Quality ACME Login with LDAP & Kerberos Agents
- CDSA/Secure Delivery
- VMS Encrypt Integration
- Kerberos & SSL version updates
- Kerberized SSH

Open Source Security Tools

- SSLDump
- SNORT for Network Intrusion Detection

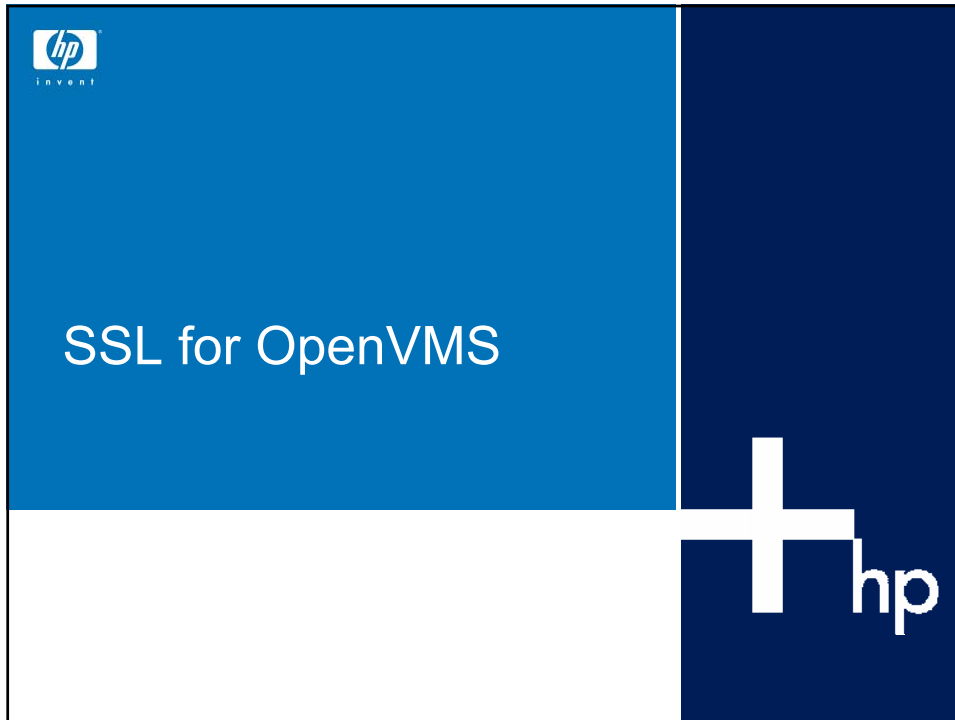
IPSEC EAK

OpenVMS V8.n (Futures)

- IPSEC ships as part of TCP/IP
- PKCS11

1G04 OpenVMS Security Update

4



The slide has a white background with a blue vertical bar on the left. In the top right corner, there is a small HP logo with the word 'invent' underneath. The title 'OpenSSL' is in a large, bold, black font. Below the title, there are two main bullet points, each followed by a list of sub-bullets. The first main bullet point is 'SSL is now a SIP with V8.3' and the second is 'SSL Startup has been added to VMS startup'. At the bottom of the slide, there is a small text string '1G04 OpenVMS Security Update' and a small number '6'.

## OpenSSL

- SSL is now a SIP with V8.3
  - SIP = System Integrated Product
  - SSL V1.3 (based on OpenSSL 0.9.7E) will be installed automatically
  - Previous versions of SSL will be removed automatically and silently
  - \$ PRODUCT SHOW HISTORY SSL will show the removal of the old SSL
- SSL Startup has been added to VMS startup
  - VMS\$LPBEGIN-050\_STARTUP.COM contains the @SYS\$STARTUP:SSL\$STARTUP invocation
  - Rename SYS\$STARTUP:SSL\$STARTUP.TEMPLATE to SYS\$STARTUP:SSL\$STARTUP.COM
  - Still need to @SSL\$COM:SSL\$UTILS manually to get foreign symbols like OPENSSL

1G04 OpenVMS Security Update 6



## OpenSSL

### • SSL now always installs on the system disk

- Even if installing as a Layered Product
- SSL\$DEFINE\_ROOT.COM no longer needed
- Rename SYS\$STARTUP:SSL\$STARTUP.TEMPLATE to SYS\$STARTUP:SSL\$STARTUP.COM

### • Differences between 0.9.7D and 0.9.7E

- <http://www.openssl.org/news/news.html>
- Fix race condition in CRL checking code.
- Fixes to PKCS#7 (S/MIME) code.

1G04 OpenVMS Security Update

7



## External Authentication





## ACME

- Authentication and Credential Management Extension (ACME) subsystem
  - New LOGINOUT and SET PASSWORD Images
  - Kerberos, MSV1\_0 and LDAP ACME Agents
  - Miscellaneous new and changed features

1G04 OpenVMS Security Update

9

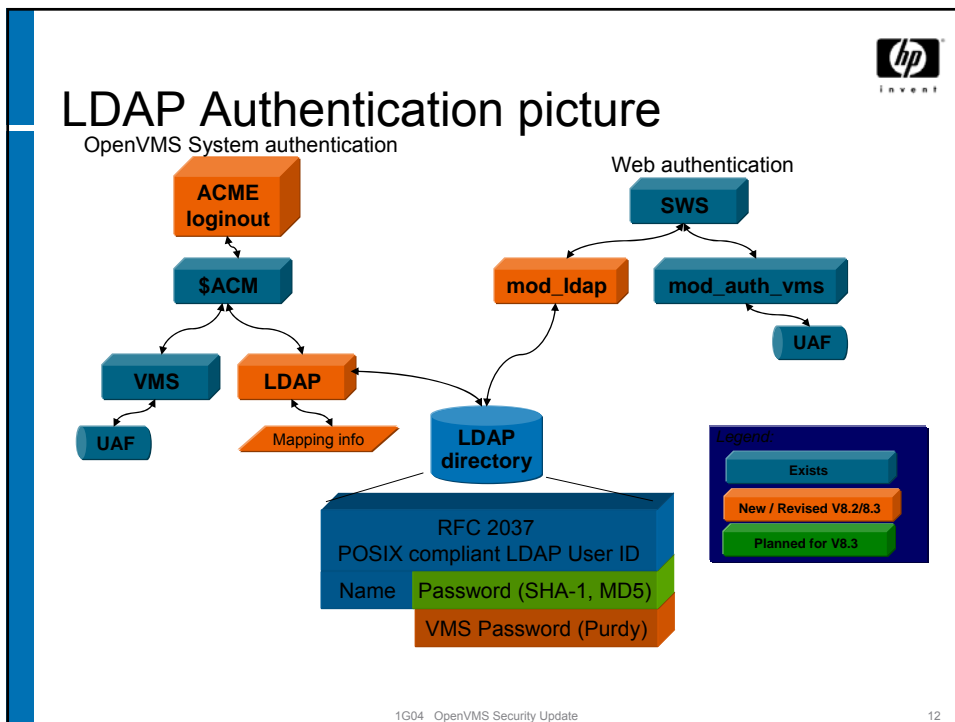
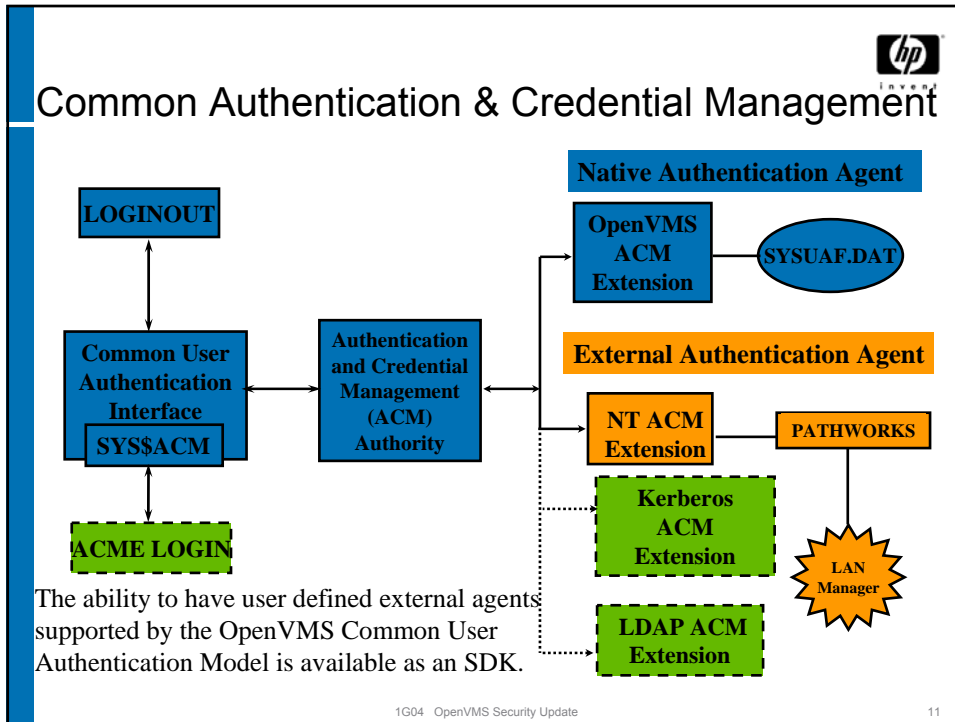


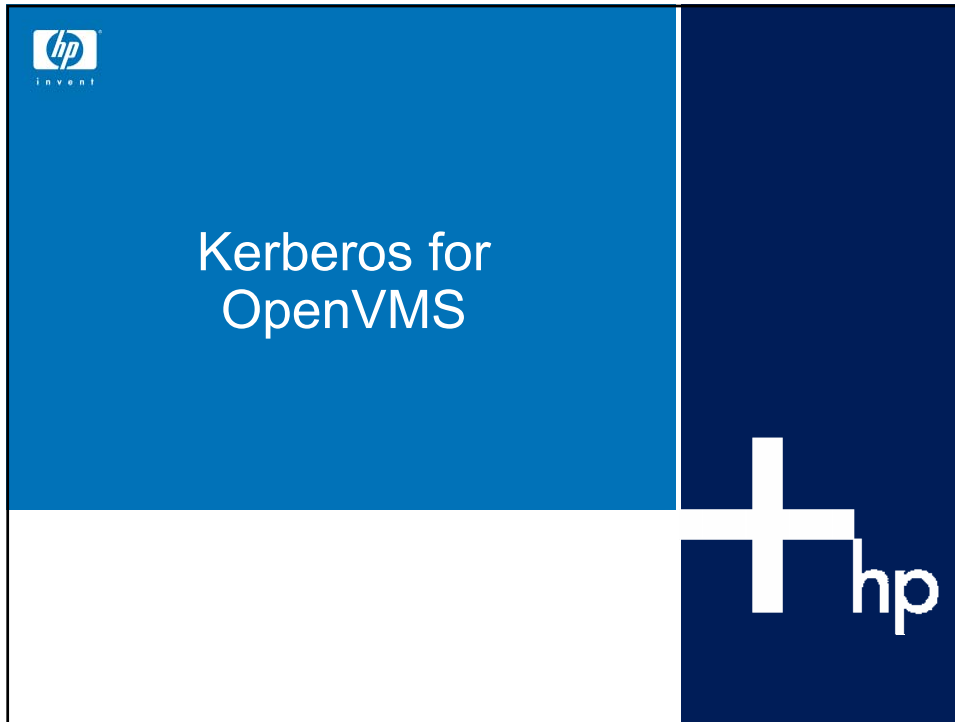
## New Loginout and Set Password Images

- LOGINOUT.EXE and SETP0.EXE images
  - Use SYS\$ACM system service and ACME\_SERVER process for authentication and password changes
- System boots with VMS ACME agent enabled
  - VMS\$CONFIG-050\_ACME\_SERVER.COM starts the ACME\_SERVER process and enables the VMS ACME agent
  - To enable other agents:
    - Edit SYS\$MANAGER: ACME\$START.COM and uncomment the desired command (Kerberos, LDAP and MSV1\_0 ACME agents in V8.3)
    - Add SET SERVER ACME/RESTART to SYSTARTUP\_VMS.COM
  - Only one ACME agent besides VMS is supported in 8.3


1G04 OpenVMS Security Update

10






## Kerberos Version Update



- Kerberos for OpenVMS V3.0 is based on MIT Kerberos 1.4.1.
  - Previous version (2.1) was based on 1.2.6
- Major differences:
  - Numerous bug fixes and minor enhancements
  - AES encryption support
  - IPv6 support (not present in the field test kit)
  - Client libraries can use TCP to connect to the KDC. This may be necessary when talking to Microsoft KDCs (domain controllers) if they issue tickets with lots of PAC data.
  - Thread-safe krb5 libraries
  - Added RPCSEC\_GSS authentication to the RPC library

1G04 OpenVMS Security Update

14



## Kerberos

- Kerberos for OpenVMS V3.0 now provides a Kerberos ACME agent
  - Allows users to acquire Kerberos credentials automatically when logging in to the OpenVMS system, without having to issue a separate “kinit” command
  - Similar functionality to the UNIX krb5\_login and pam\_krb5 utilities
  - Installed with Kerberos for OpenVMS V3.0, but must be configured prior to use
- Kerberized SSH
  - TCP/IP Services For OpenVMS V5.6 provides a new version of SSH that supports Kerberos

1G04 OpenVMS Security Update 15



## Secure Delivery for OpenVMS





## Why Secure Delivery?

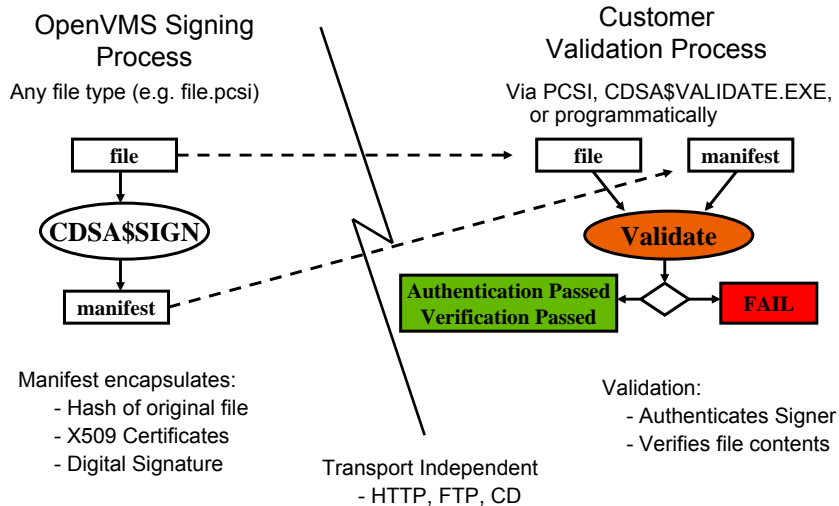
- Customers need to download kits over the Internet
  - They are nervous about web site spoofing, and other malicious activities that could compromise their security
  - Simple checksums don't provide enough protection
  - Other platforms provide better protection than what we have in the field today:
    - HP/UX uses an MD5 checksum.
    - Tru64 uses MD5 and SHA1 hashes.
    - NonStop uses some Java applet signing and software fingerprinting.
    - Microsoft platforms use Authenticode (digital signatures).

1G04 OpenVMS Security Update

17



## Secure Delivery Overview



1G04 OpenVMS Security Update

18

## Secure Delivery Overview - Design



- Secure Delivery creates digital signatures for files, so that the file and associated manifest can be delivered over an unsecured channel.
  - Delivery can be done via Internet transfers, CD/DVD distribution, or any other method of transporting a file to the end-user.
  - Secure Delivery is done automatically for SIP kits on the Itanium distribution media.
  - Two files:
    - \*.PCSI\$COMPRESSED (compressed PCSI kit)
    - \*.PCSI\$COMPRESSED\_ESW (associated manifest)

1G04 OpenVMS Security Update

19

## Secure Delivery Overview - Goals



- Secure Delivery provides a cryptographically signed hash (manifest) for any file.
  - Provides verification of the file's producer and a way to tell if the file has been tampered with
  - Primarily focused on PCSI kits for OpenVMS V8.3
  - No validation of kits will be done when installing from the Alpha CD due to space constraints
    - Validation of kits is done on both Itanium and Alpha after install/upgrade is complete.
  - There is no Secure Delivery for VAX

1G04 OpenVMS Security Update

20

## Secure Delivery – Verification tools



- Manifest verification can be accomplished:
  - Automatically, via PRODUCT INSTALL command
  - Manually, via SYS\$SYSTEM:CDSA\$VALIDATE.EXE
  - Programmatically, via CDSA\_FileValidate API
- Integrating Secure Delivery into PCSI ensures that software that is being installed on OpenVMS was not tampered with prior to installation.

1G04 OpenVMS Security Update

21

## When Does PCSI Validate Kits?




- The PCSI utility will validate kits (when a manifest is present in the source directory) for the following commands:
  - PRODUCT CONFIGURE
  - PRODUCT COPY
  - PRODUCT EXTRACT {FILE | PDF | PTF | RELEASE\_NOTES}
  - PRODUCT INSTALL
  - PRODUCT LIST
  - PRODUCT RECONFIGURE
  - PRODUCT REGISTER PRODUCT
- Kit validation checking can be turned off if necessary by use of the /OPTIONS=NOVALIDATE\_KIT qualifier to the PRODUCT command

1G04 OpenVMS Security Update

22

## Secure Delivery - A User's Perspective: Valid Manifest



\$ PRODUCT INSTALL \*

Performing product kit validation ...

%PCSI-I-VALPASSED, validation of HP-I64VMS-TEST\_THIS-0100--1.PCSI\$COMPRESSED;1 succeeded

%PCSI-I-VALPASSED, validation of HP-I64VMS-TEST\_THAT-0200--1.PCSI\$COMPRESSED;1 succeeded

The following products have been selected:


HP-I64VMS-TEST_THIS V1.0	Layered Product
HP-I64VMS-TEST_THAT V2.0	Layered Product

Do you want to continue? [YES]

1G04 OpenVMS Security Update

23

## Secure Delivery - A User's Perspective: Unsigned Kit



\$ PRODUCT INSTALL \*

%PCSI-I-CANNOTVAL, cannot validate HP-I64VMS-COBOL-0100--1.PCSI;1

-PCSI-I-NOTSIGNED, product kit was created without an associated manifest

%PCSI-I-CANNOTVAL, cannot validate HP-I64VMS-FORTRAN-0200--1.PCSI\$COMPRESSED;1

-PCSI-I-NOTSIGNED, product kit was created without an associated manifest

The following products have been selected:

HP-I64VMS-COBOL V1.0	Layered Product
HP-I64VMS-FORTRAN V2.0	Layered Product

Do you want to continue? [YES]

1G04 OpenVMS Security Update

24

## Secure Delivery - A User's Perspective: Missing Manifest



```
$ PRODUCT INSTALL TEST
```

```
...
```

```
%PCSI-W-NOVALDONE, cannot validate HP-  
I64VMS-TEST-0100--1.PCSI$COMPRESSED;1
```

```
-PCSI-W-NOMANFILE, associated manifest file  
was not found in source directory
```

```
Do you want to continue? [NO]
```

1G04 OpenVMS Security Update

25

## Secure Delivery - A User's Perspective: Invalid Manifest



```
$ PRODUCT INSTALL TEST
```

```
Performing product kit validation ...
```

```
%PCSI-E-VALFAILED, validation of PCSI$DKA0:[TEST.SD]HP-I64VMS-  
TEST-0100--1.PCSI$COMPRESSED;1 failed
```

```
-PCSI-E-CDSA_TEXT,  
CSSM_ERRCODE_MODULE_MANIFEST_VERIFY_FAILED: Modules  
manifest verification failed
```


```
%PCSI-E-S-OPFAIL, operation failed
```

```
%PCSIUI-E-ABORT, operation terminated due to an unrecoverable error  
condition
```

```
$
```

1G04 OpenVMS Security Update


26



## PCSI History and Secure Delivery

PRODUCT	KITTYPE	Operation	VAL	DATE
HP I64VMS C S7.1-13	Full LP	Install	(U)	03-NOV-2005
HP I64VMS CDSA T2.2-117	Full LP	Install	Val	25-OCT-2005
HP I64VMS DECNET_PHASE_IV X8.3-B1B	Full LP	Install	Val	25-OCT-2005
HP I64VMS DWMOTIF_SUPPORT X8.3-B1B	Full LP	Install	Val	25-OCT-2005
HP I64VMS OPENVMS X8.3-B1B	Platform	Install	Val	25-OCT-2005
HP I64VMS VMS X8.3-B1B	Oper Sys	Install	Sys	25-OCT-2005
HP I64VMS CDSA V2.1-355	Full LP	Remove	-	25-OCT-2005
HP I64VMS DECNET_PHASE_IV X8.3-AX0	Full LP	Remove	-	25-OCT-2005
HP I64VMS DWMOTIF_SUPPORT X8.3-AX0	Full LP	Remove	-	25-OCT-2005
HP I64VMS OPENVMS X8.3-AX0	Platform	Remove	-	25-OCT-2005
HP I64VMS VMS X8.3-AX0	Oper Sys	Remove	-	25-OCT-2005
HP I64VMS BLISSI64 V1.12-67	Full LP	Install	(U)	08-AUG-2005
...				
HP I64VMS TCP/IP V5.5-11	Full LP	Install		17-MAY-2005
HP I64VMS TDC_RT V2.1-69	Full LP	Install		17-MAY-2005
HP I64VMS VMS V8.2	Oper Sys	Install		17-MAY-2005


1G04 OpenVMS Security Update



## PCSI History and Secure Delivery (continued)

- Validation (VAL) types in PCSI history:
  - Empty field: validation status unknown (installed prior to Secure Delivery changes in PCSI)
  - **Val** : Kit Passed validation
  - **Sys** : Kit installed from Operating System media
  - **(U)** : Unsigned kit, not validated
  - **(M)** : Kit marked as signed, but no manifest found
  - **(D)** : Validation disabled by user
  - **(C)** : CDSA not loaded, unable to validate
  
- Values in parentheses denote abnormal conditions
  - Yes, an unsigned kit is expected to be unusual

1G04 OpenVMS Security Update



## Encryption for OpenVMS

- Layered Product for OpenVMS VAX and Alpha V6.\* & V7.\* (Required a PAK) Available on Quarterly update layered product library
- Licensed a part of OS V8.2 Alpha and Integrity (No PAK required but need to install the layered product from O/S kit LP CD)
- For OpenVMS V8.3 Encryption is bundled with the Operating System.
- (No need to install anything it's there when you install V8.3)

1G04 OpenVMS Security Update 30



## Encrypt-AES Overview

- Encryption for OpenVMS V8.3 with the Advanced Encryption Standard (AES) algorithm
- Integrating with the operating system
- Removes requirements for a separate product installation and product license
- Allows any user, system manager, security manager, or programmer to secure their files, save-sets, or application data with AES Encryption.

1G04 OpenVMS Security Update

31



## Encrypt-AES Features

- DES algorithm full function compatibility
- Encrypt-AES is integrated with BACKUP to encrypt/decrypt save-sets with AES or with DES
- Command line use of Encrypt-AES remains the same with only minor changes to qualifiers
- No new API's
- ENCRYPT\$ (API) changes are minimal: only textual parameter or flag changes are required to use AES
- Encrypt-AES supports three key sizes and four cipher modes:
  1. AESECB ! Electronic Code Book
  2. AESCBC ! Cipher Block Chaining
  3. AESCFB ! Cipher Feedback
  4. AESOFB ! Output Feedback

1G04 OpenVMS Security Update

32

## Creating/Removing AES Keys Commands



- AES keys are created with the qualifier `/CREATE_KEY /AES`  
  
`$ ENCRYPT /CREATE_KEY keyname "This is my secret key" /AES`
- Key length key must meet key length minimum maximum requirement
- Minimum number of bytes needed for the encryption or decryption operation after any ASCII key compression or byte folding (XOR). The required key sizes are as follows:
  - 128 bit mode = 16 byte key
  - 192 bit mode = 24 byte key
  - 256 bit mode = 32 byte key
- Use `/REMOVE_KEY` to delete a key from key storage

1G04 OpenVMS Security Update

33

## File Encryption and Decryption AES



```
$ ENCRYPT filename.ext KeyName -  
    /out=filename.enc -  
    /KEY_ALGORITHM=AESCBC128 -  
  
    /DATA_ALGORITHM=AESCBC128  
  
$ DECRYPT filename.enc KeyName -  
    /out=filename.dec -  
    /KEY=AESCBC128
```

1G04 OpenVMS Security Update

34

## Encrypt Reference



- New Features Manual
- Commands – DCL HELP, Messages
- Security Guide
  - overview and general information
  - AES updates
- Utility Routines - API's
- Encrypt Install & Ref. Manual (DES):
  - <http://h71000.www7.hp.com/doc/82final/6477/6477pro.pdf>

1G04 OpenVMS Security Update

35



# HP Secure Server





## HP Secure Server - Review

- Secure web-based e-mail server solution
- Works anywhere there is an Internet connection and a compatible browser (Firefox, Safari, Opera, IE)
- Based on OpenVMS and powered by Quintara® software from Brilliant Systems
- Built-in attachment virus scanning, anti-spam, external delivery functions
- Integrity and Alpha servers, packaged with hardware or software-only
- Available today

1G04 OpenVMS Security Update

37



## HP Secure Server - New Features

- Many exciting new capabilities
  - + Personal calendar
  - + Spell checking on message compose
  - + Drafts folder
  - + Enhanced attachment support (4 instead of just 1)
  - + More address book import/export features
  - + POP3 compatibility mode for easier migration
  - + Copy to folder capability
  - + External delivery of valid messages to PDAs and cell phones now supported on HP TCPIP Services

1G04 OpenVMS Security Update

38



## HP Secure Server

<http://trysecureserver.com>

1G04 OpenVMS Security Update

39

