# CA Deliver™

## Release Notes

### r11.6

# CA Technologies Product References

This document references the following CA products:

- CA ACF2™
- CA Top Secret®
- CA View®
- CA Mainframe Software Manager (CA MSM)

# Contact CA Technologies

**Contact CA Support**

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

**Providing Feedback About Product Documentation**

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

# Contents

# Chapter 1: Overview

This document provides information about the new encryption function in CA View -- a companion product to CA Deliver r11.6 -- and any information about how this feature might affect CA Deliver r11.6.

It also includes the supported environments and how to use this document in conjunction with the existing documentation set.

**Important!** Be aware that CA Deliver r11.6 is built on CA Deliver r11.5, and this document includes only a description of the changes or updates that are directly connected to encryption in CA View and use of ESD PAX or MSM installation, and global version number changes; therefore, with the exception of the information contained in this document and the Installation Guide, all pre-existing product documentation is accurate and timely.

This section contains the following topics:



## Data Encryption with CA View

Protecting your data is of utmost importance. Customers that store credit card data must abide by PCI compliance. One of the most important factors in this compliance is to provide optimum security–*data at rest must be encrypted via strong encryption.*

These sections explain what happens during the encryption process and provide brief definitions of the new terms you may encounter.

### Encryption Keys and the CA View Database

If you are using CA Deliver with CA View, be aware that we are integrating with the IBM CPACF and ICSF services for encryption. You activate encryption using a simple CA View initialization parameter. The process is as follows:

1. Based on a client-specified interval, key labels and encryption keys are automatically written to the ICSF Key Store Data Set (CKDS).
2. A Call is sent to ICSF to obtain a proper key.
3. CPACF or ICSF is invoked to perform the AES encryption.

**Important!** If you are sharing the ICSF CKDS data set between multiple z/OS systems, the ICFS SYSPLEXCKDS(YES,FAIL(*xxx*)) parameter MUST be specified in the ICFS installation options data set.

This allows newly created keys to be shared with other running ICFS systems. Without this parameter, the ICSF in-memory copy of the CKDS will be out of sync between the systems; this results in reports being encrypted with one key and later incorrectly decrypted with another key. When this occurs, the original keys are replaced with keys from another system. *Reports using the original keys can no longer be decrypted.*

Be aware of the following:

- When the encryption feature is enabled, all report and index data will be encrypted on both disk and tape.

  This includes the CA View database, backup, duplex, DR (Disaster Recovery), and unload tapes.
- Existing backup tapes can be encrypted by using the CA View SARPAC utility.
- Reloading an older report back to disk will automatically encrypt the disk copy.
- Copying the database will encrypt all reports on the copied database.

**Note:** See Supported Cryptographic Hardware (see page 8), Encrypt the Data (see page 9), and Encryption and Decryption Software Considerations (see page 9) for more information.

**Important!** CA View *does not keep* a local copy of the encryption key; it stores a clear 256 bit encryption key in the ICSF Key store (CKDS). CA View only accesses the CKDS via the ICSF services – it does not require any security permissions to access this data set. We recommend that you use your external security package to prevent unauthorized browsing of the CKDS data set.

Currently CA View uses ICFS as a key store. Future releases will provide support for other third party key managers including any CA products that provide this functionality.

## Supported Cryptographic Hardware

Two cryptographic hardware choices are available for use on various systems:

- Cryptographic Coprocessor Facility (CCF) A standard component on z900 and a no-cost option for z800. On z800 and z900 systems, ICSF requires CCF.
- CP Assist for Cryptographic Functions (CPACF) A standard component on z9 and z10 and a no-cost option for z890 and z990

Other available cryptographic hardware components do not necessarily improve encryption performance, as described in the following list:

- Peripheral Component Interconnect (PCI)-based coprocessors (PCICC, PCIXCC, and Crypto Express2), which provide secure key storage, hardware hashing, and SSL support.
- PCI-based accelerators (PCICA, Crypto Express2 configured in accelerator mode), which provide high performance SSL assistance.

**Note:** Because CA View uses a clear key, it does not require the use of the Cryptographic Express2 coprocessor (CEX2C). To run ICSF without a CEX2C coprocessor, you will need ICFS release FMID HCR7751or higher.

If you are running an older release of ICSF, you will be required to purchase a CEX2C coprocessor because older releases of ICSF required that hardware to initialize the CKDS data set.

## Encrypt the Data

Encryption is enabled by the SARINIT parameter ENCRYPT=NO|ICSF,*nnn.*

See the CA View documentation for more information.

## Encryption and Decryption Software Considerations

Be aware that if you use z/OS software encryption and decryption, the time the CPU uses to encrypt or decrypt data will increase the CPU time consumed by the job or started task.

## What Gets Encrypted

In CA View, all report data and report index data get encrypted. Panels, banner pages, and resource data is not encrypted.

# Environment

This section discusses the current operating systems supported, scalability, compatibility, and the security interfaces.

## Supported Operating Systems

The minimum software required to run this release of the product and meet the performance requirements is IBM z/OS 1.9 and higher.

## Scalability, Availability, and Prior Versions

CA Deliver r11.6 will have the same scalability as previous versions.

Availability should be almost 24x7 except for periodic maintenance which will vary in frequency according to the needs of your site.

Note the following:

- If you are also using CA View, CA Deliver allows concurrent archiving to release 11.0, r11.5, and r11.6 CA View releases.
- The r11.6 XMS and DRAS tasks allow concurrent viewing of release 11.0, 11.5 and 11.6 CA View databases.

## Backward Compatibility

CA Deliver r11.6 through CA View will be able to read prior versions of report data found on disk and tape.

**Important!** CA View r11.6 encryption does not have backward compatibility to allow previous releases to access encrypted data. Once you start to use encryption, you cannot read the encrypted tapes in a prior release.

See your CA View documentation for more information.

## Security and Privileges

Reports are secure after encryption. We are using AES encryption with 256 or 128 bit keys.

External security interface is provided to CA Top Secret, CA ACF2, and IBM RACF.

## New Messages

**RMODBV06**

**Database successfully versioned to *release***

**Reason:**

The database has been successfully versioned to the requested release level.

**Action:**

None. This is an informational message.

**RMOSVR05**

**CSVDYLPA macro failed for module xxxxxxxx, R15=xxxx R0=xxxx FLAGS=xxxx PROCESSING CONTINUES**

**Reason:**

RMOSVR was unable to add the above module to the MLPA CDE directory.

**Note:** This is only needed by product support and does not affect normal product performance.

**Action:**

Contact CA Technical Support.

**RMOSTC80**

**CSVDYLPA macro failed for module xxxxxxxx, R15=xxxx R0=xxxx FLAGS=xxxx PROCESSING CONTINUES**

**Reason:**

RMOSTC was unable to add the above module to the MLPA CDE directory.

**Note:** This is only needed by product support and does not affect normal product performance.

**Action:**

Contact CA Technical Support.

## Terminology

You may encounter the following terms and abbreviations in this documentation and the CA View documentation set:

- AES – Advanced Encryption Standard
- Asymmetric key – A different key is used for encryption and decryption. Thought of as a public key and a private key.
- CKDS – ICSF Cryptographic Key Data Set is the storage vehicle for symmetric keys
- CPACF – CP Assist for Crypto Functions
- DSS – Data Security Standard
- IBM CPACF and ICSF services
- ICSF – Integrated Cryptographic Service Facility
- MSM – CA Mainframe Software Manager
- PAX – UNIX file system archive file
- PCI – Payment Card Industry
- PCI compliance – Meeting the standards that were created to help organizations that process card payments by preventing credit card fraud through increased controls around data and its exposure to compromise
- Symmetric Key – Same key is used for both decryption and encryption

# Global Changes for Release 11.7

Be aware of the following changes that appear throughout this documentation set:

- HBB6 is changed to HBB7
- EB6 is changed to EB7
- XMB6 is changed to XMB7
- SAMPJCL contains the following non-MSM install JCL members:

  BRNAREAD, BRNEDALL, BRNSEDIT, BRN1ALL, BRN2CSI, BRN3RECD, BRN3RECT, BRN4APP, BRN5ACC, BRN6RECP, BRN7APYP, BRN8ACCP
- CVDEOPTN contains the following customization JCL members:

  HBRNADDS, HBB7ATHT, HBB7ATHX, HBRNBLOD, HBB7BPCX, HBB7BPTX, HBRNCAPF, HBRNCONV, HBB7DFMT, HBB7DSCX, HBB7FSSX, HBB7JCLX, HBB7JS2X, HBB7J2X, HBB7J319, HBB7J321, HBB7J323, HBRNOLOD, HBB7OMSX, HBB7PRBX, HBB7RECX, HBB7RPTX, HBB7RPX, HBB7RRQX, HBB7SMFX, HBB7SUBX, HBB7USAX, HBB7USRX, HBB7USTX, HBB7USXX, HCB7CICX, HCB7IMSX, HCB7ROSX, HCB7SPFX, HCB7TSOX, HCB7XCTR, HBRNVERS

# Chapter 2: Installation and Upgrade

CA Deliver is installed using the MSM, ESD PAX process, or tape.

For the CA Deliver installation steps see your CA Deliver Installation Guide and Upgrade Considerations in this guide.

## The ESD PAX Installation Process

You can obtain CA Deliver in a compressed format (pax.Z file) that enables you to install directly from DASD. This is known as the ESD PAX process.

To install CA Deliver using the ESD PAX process, see your r11.7 documentation.

## Upgrade Considerations

CA Deliver Release 11.7 is available to all CA Deliver customers with active maintenance contracts. There is no specific license required to upgrade to release 11.7.

**Note:** If you are using the companion product CA View, release 11.7 of CA Deliver is backward compatible with CA View Release 11.0, Release 11.5, and Release 11.6. XMS and CA Deliver direct archival can concurrently browse or archive to CA View 11.6, 11.5, and 11.0 databases.

For upgrades from CA Deliver Release 11.6 to Release 11.7, you must make sure that PTF RO30477 is applied to your CA Deliver Release 11.6 system prior to upgrade. PTF RO30477 is required to ensure the integrity of the Release 11.7 SMP/E environment during the upgrade process.

See Backward Compatibility for information about encryption compatibilities.