
Advanced Software Products Group, Inc.www.aspg.com

Deploying high-performance cryptography to resolve emerging security mandates for CA IDMS™ databases



Cryptography for CA IDMS™ Databases


Copyright © 2018 ASPG, Inc. All rights reserved. MegaCryption and MegaCryption-IDMS are registered trademarks of ASPG, Inc. Trademarks of other companies or products mentioned herein are for identification purposes only and are the property of their respective companies.

Advanced Software Products Group, Inc.www.aspg.com

Today's Presenter:

Greg Thomason
greg.thomason@aspg.com
239-649-1548





Advanced Software Products Group, Inc.
www.aspg.com

Adding cryptography to existing operations

- Review mandates. Identify affected operations and resources.
- Coordinate appropriate resolutions to use cases.

- Evaluate then select an appropriate cryptography system.
- Roles: Admins, Programmers, Key managers, Cryptographers
- Configure and integrate cryptography routines/utilities into apps, databases, procs, exits, scripts, etc.


Advanced Software Products Group, Inc.
www.aspg.com


Introduction To MegaCrypton on z/OS


Features


- Cryptography
- Key management
- Hashing
- Digital Signatures
- Compression
- Text reformatting

Interfaces

- Batch Utilities
- Cryptography API
- ISPF Application
- Sample JCL Procs
- IDMS, DB2, IMS exits
- Sample Applications




 Advanced Software Products Group, Inc. www.aspg.com




- Comprehensive solution to encrypt sensitive IDMS data.
- Easy to install and configure.
- Ability to encrypt **entire records*** (Record Mode) and **individual fields** (Data Mode) in a record.
- Transparent to applications; no application changes.
- Supports AES-128, AES-256, and 3DES algorithms.
 - Cryptography accelerators are utilized when available.


* In Record mode, only data outside the control section of the record is encrypted.

 Advanced Software Products Group, Inc. www.aspg.com

Installation

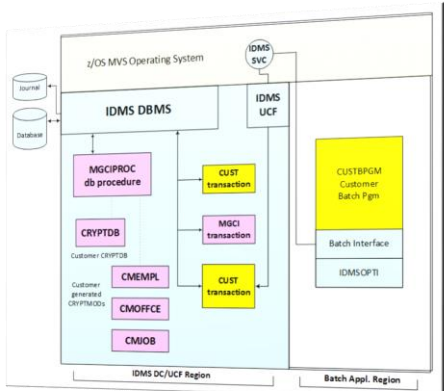
- Software installed via SMPE.
- Apply product activation code.
- Add installation load libraries to IDMS regions and Local Mode batch jobs.
- Define MGCI to IDMS via Sysgen (System Generation).






Advanced Software Products Group, Inc.
www.aspg.com

Configuration

- Identify data to encrypt.
- Create CRYPTDB to identify the databases being encrypted and how to locate the encryption key.
- Create CRYPTMOD describing data to be encrypted.
- Modify the schema to call the MGCIDMS database procedure.
- Run conversion utility to perform initial encryption.







Advanced Software Products Group, Inc.
www.aspg.com


Key Management

Three key storage options are provided.

- Store keys in the CRYPTDB module (for testing only).
- Save keys in an access-protected data set.
- Store keys in a SAF keybox (recommended).


- ✓ Role-based separation of duties.
- ✓ Protected from unauthorized use and modification.
- ✓ Prevent in-clear recovery of keys.
- ✓ SAF auditing.





Advanced Software Products Group, Inc.
www.aspg.com

How It Works


- At IDMS region startup, the initialization routine loads the modules **CRYPTDB** and **CRYPTMOD** into memory, validates them, and locates the encryption keys. Any errors are reported in the IDMS log and may disable encryption.
- When the MGCIIDMS database procedure is invoked at run time, it uses the information passed to it by IDMS, and the information loaded into memory at startup to control the cryptography.
- In Local Mode processing, the first time the database procedure is called, it recognizes that it is running in Local Mode and performs the initialization processing at that time.





Advanced Software Products Group, Inc.
www.aspg.com

Utility Functions Provided


- Batch Conversion Utility MGCICONV provides:
 - Encryption and Decryption
 - Key Rotation
 - Display
- Online Utility provides:
 - Display current configuration
 - Temporarily disable encryption updates for a database
- Initialization Utility can be rerun manually to load a new configuration.





Advanced Software Products Group, Inc. www.aspg.com

Special Considerations

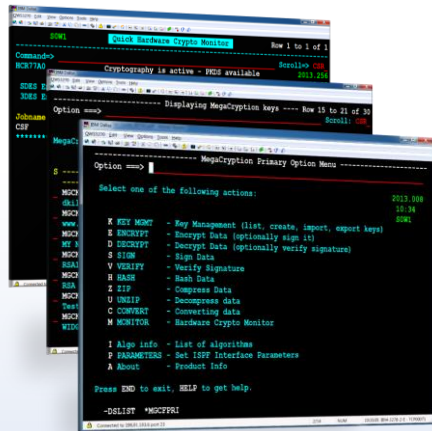
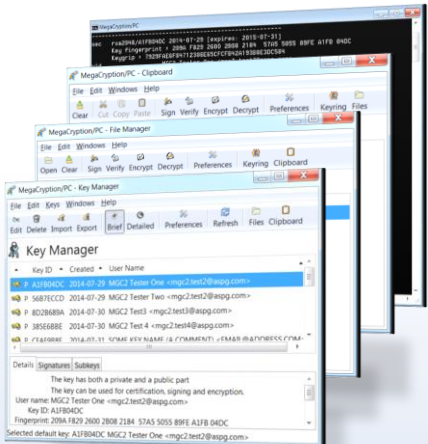
- **CALC Keys**
 - Encryption CALC keys is fully supported, but additional configuration is required.
 - Additional encryption calls at run time required.
 - If duplicates allowed and order is important, then user may need to perform the initial encryption, because the conversion utility will not maintain duplicate order.
- **Sort Fields**
 - Limitations - works ok if sort field is used as a full alternative key to finding the record.
 - Partial Key searches are not supported. Application changes may be required.
- **Full support for compression of encrypted data**
 - Record Mode - compress then encrypt; decrypt then decompress.
 - Data Mode - encrypt then compress; decompress then decrypt (because we have no way of finding the field to encrypt after it is compressed).





Advanced Software Products Group, Inc. www.aspg.com

Other MegaCrypton Software

Enterprise Cryptography Suite for z/OS, Windows, Linux, Unix







Advanced Software Products Group, Inc.
www.aspg.com

Contact ASPG today: 239-649-1548

"I would recommend MegaCryption because it does what it says, handles our current needs and future needs that will arise, has more functions than other products, and the cost of the product was great. I would rate the technical support as a 10."

- Major Northeast University







Copyright © 2018 ASPG, Inc. All rights reserved. MegaCryption and MegaCryption-IDMS are registered trademarks of ASPG, Inc. Trademarks of other companies or products mentioned herein are for identification purposes only and are the property of their respective companies.

Please Complete a Session Evaluation Form

- The number for this session is **D12**
- After completing your session evaluation form, place it in the envelope at the front of the room


IUG / CA IDMS Technical Conference Session Evaluation Form


Session Number: _____ Name (Optional): _____

Session Title: _____

Rate the overall session	Poor	Fair	Good	Excellent
Rate the overall session	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

	Strongly Dislike	Dislike	Neutral	Like	Strongly Like
The speaker was prepared and knowledgeable of the subject covered	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Comments:					
The session met my expectations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Comments:					
The material is valuable to my current job	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Comments:					
I would recommend this session to a colleague	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Comments:					
The session length was appropriate for the content	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Comments:					
My session could be useful as a reference	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Comments:					
General Comments:	<div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div>				