

PCI DSS REQUIREMENTS AND CA PRODUCTS:

CA ACF2™ Option for DB2® CA Top Secret® Option for DB2®

The CA Option for DB2 allows you to control the security of your critical DB2 for z/OS environment where it's most practical: within the existing CA ACF2™ or CA Top Secret® access control system.

PCI Requirement 7.1.4

Confirm that access controls are implemented via an automated access control system.

PCI Requirement 7.2.1

Confirm that access control systems are in place on all system components.

[Emphasis added.]

How the Option for DB2 Address this Requirement:

If you have CA ACF2 or CA Top Secret, you are already running an automated access control system.

The CA DB2 Option for your principal security tool brings your DB2 sub-system under the management of your existing, professionally-managed access control environment.

PCI Requirement 8.1

Assign all users a unique ID before allowing them to access system components or cardholder data.

PCI Requirement 8.5.8

Do not use group, shared, or generic accounts and passwords.

How the Option for DB2 Address this Requirement:

Native DB2 security requires that individual users be granted access to resources. To simplify their workload, DB2 DBAs commonly employ "secondary authorization" or "group" IDs.

Neither CA ACF2 nor CA Top Secret requires this approach. Using the Option for DB2 brings access security under control of a mechanism that was designed to be secure *and* easily managed from the start, without the need for secondary authorization or group IDs.

Additional Considerations

PCI DSS REQUIREMENT NUMBER	PCI DSS REQUIREMENT AREA	SUPPORT BY CA OPTION FOR DB2
10.1, 10.2, 10.2.1	Audit Trails	Native DB2 audit trails that link primary and secondary IDs require resource-intensive tracing that is often omitted. The CA Option for DB2 incorporates your existing CA ACF2 or CA Top Secret audit trail and reporting facilities.
6.3.6	Removal of Special Accounts in Production	In the production environment, special DBA group accounts such as "DBADM" may only exist in order to grant access privileges for end users. This could be interpreted as a violation of the "custom application accounts" provision. Because neither CA ACF2 nor CA Top Secret requires these group accounts to facilitate ownership, this is not an issue once you employ the CA Option for DB2. Under this Option, special group account access is allowed only when truly required. In addition, by using the logging option on these highly privileged user accounts a full audit trail is available for on-going monitoring and reporting.
12.5, 12.5.5	Assignment of Security Team to Monitor and Control Access to Data	A common audit finding in all compliance reviews is the so-called "Separation of Duties" issue. In the DB2 arena this often applies to the removal of the security function from the DBAs to the security team, where it truly belongs. The requirements identified by number here may be similarly interpreted as they require the assignment of a security team to monitor and control access to <i>all</i> data, presumably including the critical DB2 tables. If your security team already utilizes CA ACF2 or CA Top Secret and must now manage the DB2 environment, it makes sense to use their existing controls and administrative tools. The CA Option for DB2 does exactly this.
6.2	Subscribe to Alerts	You may subscribe to all alerts at support.ca.com. After logging on, expand the Subscriptions link on the left, and select the Hyper Subscriptions drop-down.

The CA ACF2 or CA Top Secret Option for DB2 moves access security control away from the DBA team and to the existing access security infrastructure at your organization. The use of this product addresses common "separation of duties" issues, and the specific PCI concerns expressed above. Moreover, the product includes a migration tool to convert your current native DB2 security environment.

By using the Option for DB2 for either CA ACF2 or Top Secret, users have the ability to migrate the critical DB2 infrastructure to a more professionally managed security environment.

Legal

Copyright © 2008 CA. All rights reserved. DB2 and z/OS are trademarks of International Business Machines Corporation in the United States, other countries, or both. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. THIS DOCUMENT IS FOR YOUR INFORMATIONAL PURPOSES ONLY. TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT WILL CA BE LIABLE FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENT, INCLUDING, WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED OF SUCH DAMAGES. **Notwithstanding anything in this publication to the contrary, this publication shall not: (i) constitute product documentation or specifications under any existing or future written license agreement or services agreement relating to any CA software product, or be subject to any warranty set forth in any such written agreement; (ii) serve to affect the rights and/or obligations of CA or its licensees under any existing or future written license agreement or services.**

Source Document

The source for this document is the PCI DSS version 1.2, published in October 2008, as this was the current standard at the time of this writing. A free copy may be obtained at the PCI Security Standards Council ([HTTPS://WWW.PCISECURITYSTANDARDS.ORG/](https://www.pcisecuritystandards.org/)).