



zedSuite

Zed E-Commerce and WebCRM 7.5

Release Notes

11/29/2011



eBusiness Solutions for SAP



PA-DSS 2.0 Validated

What is PA-DSS? (Payment Application Data Security Standard)

The global security standard created by the [Payment Card Industry Security Standards Council](#) (PCI SSC). ^[1] PA-DSS was implemented in an effort to provide the definitive data standard for [software](#) vendors that develop payment applications. The standard aims to prevent developed payment applications for third parties from storing prohibited secure data including [magnetic stripe](#), [CVV2](#), or [PIN](#). In that process, the standard also dictates that software vendors develop payment applications that are compliant with the Payment Card Industry Data Security Standards ([PCI DSS](#)).

To whom does it apply?

The PA-DSS applies to software vendors and others who develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement, where these payment applications are sold, distributed, or licensed to third parties.



PCI and PA-DSS

Use of a PA-DSS compliant application by itself does not make an entity PCI DSS compliant, since that application must be implemented into a PCI DSS compliant environment and according to the PA-DSS Implementation Guide provided by the payment application vendor.



Changes required for validation

- Storage and handling of credit card details
- Encryption
- Logging
- User Authentication
- Plug-in available to force use of https for all login, account details, and checkout traffic
- Application or server level security against sql injection, cross-site scripting, buffer overflows



Storage and handling of credit card details

Storage of the credit card number, CVC(card verification code) in the e-commerce and webcrm database has been removed.

During checkout, credit card details are encrypted using dynamic encryption and only stored in web server session memory. After checkout completes or times out from inactivity, the data is removed.

Wallet functionality(ability for customer to store payment information in their profile) has also been removed. Each time a customer checks out they will need to enter their credit card data, or choose another payment method.



Encryption

Private keys are no longer used for data encryption in either the installer, synch manager or API. PA-DSS requires that at no time is a key stored in plain text, no one person can know the entire key, and in the event of a personnel change all keys must be changed.

Users passwords are hashed

Instances.xml connection strings are encrypted using dynamic key

Web.config connection string is still optionally encrypted per choice during instance creation using IIS encryption

Session cookies are encrypted



Logging

Enhanced logging of user and super user actions and changes to system configuration.

- Order placed
- Bad password
- Account locked out
- Role definition changed and assigned
- Credit Card Gateway config changed
- Log viewed
- Password changed



User Authentication

Requirement of strong passwords, inactivity timeouts, and password expiration for all users.

Unique userids are enforced. No two users can use the same userid for login

The value for email address is no longer read during login. A user can only use their email address for login when it is entered into the userid field when creating a new account



User passwords and synchronization

Internal B1 users passwords are no longer displayed in plain text in a UDF in B1 and are not synchronized to B1.

Business Partner Contact passwords are not updated in B1 after they have been changed in E-Commerce.

Random passwords are assigned to Bp Contacts and Internal users upon initial synch.



User passwords and synchronization

All users passwords can be changed by a super user, or with the “Reset User” program

After a user logs in for the first time, or after their password has been changed by the Reset User tool, they will have to choose a new, strong password.

Bp Contacts passwords can be set before the initial synch, after they login for the first time, a password change is required.

Basically the requirement from PA-DSS is that at no time is any users password stored in plain text, and is only known to the user.



Upgrades

Card numbers, expiry and CCV

- Installer will decrypt, update using new dynamic key, then overwrite 3x to ensure original data is not retrievable via data forensics

Users passwords are decrypted and then re-encrypted to one-way hash

Private key is removed from instances.xml after data has been upgraded

Web.config is recreated with private key removed

Synch manager does not do any encryption, private key is removed from synchconfig.xml during upgrade step of running a synch



Compatibility

Solution Component	Compatible	Notes
SAP Business One 8.8.1 PL9	Yes	
SAP Business One 8.8 PL22	Yes	
Windows Server 2003 SP2 32-bit with IIS 6	Yes	64-bit was not tested, however no 64-bit related issues found with Server 2008 64-bit
Windows Server 2008 R2 64-bit with IIS 7.5	Yes	
Windows 7 (any edition) 32 or 64-bit with IIS 7	Yes	
Windows Vista 32-bit or 64-bit with IIS 7	Not tested	This was not tested, however, as Server 2008 uses IIS 7, there should not be any issues
Windows XP SP3 32-bit or 64-bit with IIS 5.1	No	
SQL 2005 32-bit*	Yes	64-bit was not tested, however no 64-bit related issues found with Server 2008 64-bit
SQL 2008 R2 64-bit*	Yes	
Google Chrome 10	Yes	
Firefox 8	Yes	
Internet Explorer 8 and 9	Yes	Version 8 may have minor display issues in the Admin
Apple Safari 5	Yes	



Changes

Removed field for private key on instance list screen

Removed private key from instance records in instances.xml

Removed private key from web.config

Delete verification code from userswallet and orderpayment tables

Drop userswallet table

Disable Back and Upgrade buttons while upgrade or installation is in process

Updated icon for system task bar and title bar, desktop shortcut, and start menu item

Added password validation to Reset User

New background image in setup.exe program

Remove private key parameter from NPAccount constructor

Removed max user functionality from My Account >

Fixed issue where order confirmation emails weren't being sent if account had more than 500 orders

Fixed issue where order confirmation email error prevents remaining emails from sending

Fixed issue where Messaging service does not work and throws event log error (object reference error) upon startup

Commas not allowed in usernames

Functionality to prevent password re-use added

Implemented password expiration

Prohibit auto-complete on password field on login.aspx

Users must change password upon first login

Queueing BP with Add multiple times will duplicate tax exemption records



Changes

All passwords are reset upon forgot password request, removed config option

Creating an account also now logs user in

Prevent RedirectTo URL parameter from redirecting to external page

Insecure webflow will redirect to non-SSL

Prevent login and checkout pages from caching in the browser

Webflow entries now trim trailing spaces

Require that passwords contain at least one non-numeric character

Users can no longer login with email address, only userid(which could also happen to be their email address)

Removed password fields from user edit screen on my account section

Removed username from change password screen

Not syncing passwords back to B1

Fixed issue with deleting user

Fixed issue with renaming contact

User can request password using userid

Logout deletes all session data

Including plug-in to enforce https on all login, checkout, my account pages

