dbsign™
Data Security Suite

DBsign for HTML Applications Version 4.0 Release Notes

Gradkell® Systems Inc.

Version 4.0

Copyright Notice:

Table of Contents

1.0 What's New

1.1 New Client Software: The DBsign Universal Web Signer

The DBsign Universal Web Signer (UWS) is our new client-side signing solution that is based on cross-platform technology. The UWS has many important features:

- **Zero deployment.** Since the UWS runs inside the web page (like an image or flash animation) it does not need to be installed on each client workstation.
- **Auto-Updating.** When the host application decides to use a newer version of the UWS, only the UWS download location needs to be specified on application pages that use the UWS. All clients will automatically start using the newer version.
- **Supports Multiple Hardware and Operating System Platforms.** The DBsign UWS supports 32 and 64 bit browsers and operating systems such as Microsoft Windows XP and higher, Apple OSX 10.4 and higher, Linux, and more.
- **Fully Scriptable in All Supported Browsers.** The DBsign UWS can be accessed programatically by scripting languages such as Javascript on Microsoft Internet Explorer, Mozilla FireFox, Apple Safari, and others. This allows modern web applications to make user signing operations more efficient and user friendly.
- **Application Isolation.** The DBsign UWS allows applications to have complete control of their configuration management. That is, if a given user accesses many different DBsign enabled applications, each application can use different versions of the UWS and each application has their own set of client-side configuration options.

1.2 More Platform Support

Both the DBsign UWS client and the DBsign Server have increased multi-platform support.

The DBsign UWS supports most 32 bit and 64 bit desktop platforms including

- Microsoft Windows XP and higher,
- Apple OSX 10.4 and higher,
- Linux, and

- others.

The DBsign Server supports 32 or 64 bit versions of

- Microsoft Windows XP or higher,
- Microsoft Windows Server 2003 and higher,
- Apple Mac OSX Server,
- Sun Solaris (SPARC or x86),
- Linux and
- others.

1.3 New Cryptographic Subsystem

In DBsign 4.0, both the DBsign UWS client and the DBsign Server benefit from a redesigned, multi-platform, high-performance cryptographic subsystem. Although the new cryptographic subsystem has features similar to the DBsign 3.0, the new system is even more efficient and much more flexible. The new DBsign 4.0 cryptographic subsystem

- supports more **message digest algorithms** (cryptographic hash algorithms) including MD5, SHA-1, SHA-256, SHA-384, and SHA-512,[1]
- supports PKCS #12, PFX and Java JKS key files,
- supports **operating system specific cryptographic subsystems** including Microsoft CryptoAPI and Apple OSX Keychains (including smart cards and other devices),
- supports **hardware cryptography** via PKCS #11 (e.g., smart cards, cryptographic tokens, high performance cryptographic accelerators, etc.),
- supports **Network Security Services** (NSS) on all supported platforms for high performance, multi-platform, FIPS 140-2 validated cryptography with the speed of native machine code,
- supports **FIPS 140 validated cryptographic modules** including the DoD Common Access Card and PIV cards,
- has even more **efficient support for CRLs, OCSP, and CRL-DP**, and
- passes all applicable **interoperability and security tests** in the NIST PKITS test suite.
- Complies with the requirements outlined in the **DoD Digital Signature Guidelines**.

1 DBsign 4.0 fully supports MD5, SHA-1, SHA-256, SHA-384, and SHA-512. These digest algorithms are supported in digital signature and verification operations (i.e., signing/verifying documents and data by the end user) as well as certificate path validation (i.e., DBsign 4.0 supports the validation of certificate paths in which CAs have issued certificates signed with any or all of these digest algorithms).

1.4 Important Third Party Security and Interoperability Certifications

DBsign 4.0 has undergone rigorous testing and evaluation by independent third parties.

- **NIAP Common Criteria Validation.** The Common Criteria is an internationally recognized set of security evaluation criteria that was developed by the National Security Agency (NSA). It replaces the older Trusted Computing Security Evaluation Criteria (TCSEC, aka, the "Rainbow Series", or "Orange Book"). DoD directive 8500.1 mandates that all security products used in DoD be validated under the Common Criteria. DBsign was the first and is still the only digital signature product to be NIAP Common Criteria Validated. DBsign 4.0 is also the first and currently the only digital signature product to be validated against DoD's Protection Profile for Public Key Enabled Applications which outlines the security requirements for applications which use PKI technologies.
- **DoD Joint Interoperability Test Command PKE Interoperability Certification.** DBsign has been certified through JITC PKE interoperability validation multiple times, each time passing with zero defects. DoD JITC PKE certification ensures that DBsign is fully interoperable with DoD's Public Key Infrastructure. A major component of JITC PKE testing is the NIST Public Key Infrastructure Test Suite (PKITS), which ensures that DBsign correctly performs certificate path validation according to the relevant security standards.

1.5 Significant Performance Enhancements

The DBsign Server 4.0 is able to achieve higher performance under heavy load environments due to greater multi-threaded concurrency and a more efficient caching architecture. These performance improvements are largely derived from the new cryptographic subsystem.

1.6 Certificate Status Caching

DBsign's Certificate Status Caching (CSC) is another performance enhancement which can greatly improve performance of heavily loaded systems, especially those which rely on OCSP and CRL-DP for revocation status checking. For example, application owners may decide that a certificate's revocation status does not need to be checked more often than, say, every 20 minutes. When DBsign's CSC is enabled, the last revocation status is cached and a maximum revocation check frequency is enforced which ensures that an individual certificate's revocation status is not checked too frequently. This eliminates unnecessary and costly network round trips to OCSP responders and CRL-DP

sources and, in some circumstances, can greatly improve application performance. If the DBsign CSC is disabled (the default), DBsign checks the revocation of all certificates each time they are used in a security operation.

1.7 Application Session Tokens

Application Session Tokens (AST) allow host applications increased document level security by giving the host application the ability to allow only specific users to digitally sign specific documents during a specific time period. Essentially, the AST feature allows the DBsign Server to be "linked" to the application's login session in a application server independent manner.

1.8 CRL Updater

DBsign 4.0 handles CRL retrieval much differently than DBsign 3.0. In DBsign 3.0, DBsign would automatically retrieve the CRL from an LDAP directory when the CRL reached its nextUpdate date. However, many DBsign customers require a more frequent CRL update period to achieve their revocation information "freshness" policies. This fact, in combination with customer changes in CRL access methods (e.g. HTTP instead of LDAP) mandated a change in DBsign's CRL retrieval mechanisms. In order to meet customer requirements, DBsign 4.0 no longer automatically retrieves CRLs but includes the CRL Updater Utility program that allows the host application to "push" CRLs to DBsign. The CRL Updater is designed to be used by application batch mode scripts that run at a certain frequency. The CRL Updater is configured by a standard DBsign configuration file that can be edited by DBsign 4.0's new graphical configuration file editor.

1.9 Graphical Configuration File Editor

DBsign 4.0 uses a new XML based configuration file format. The format is easily edited with a text editor, however, DBsign 4.0 also includes a graphical editor that greatly simplifies configuring the DBsign Server, Admin Tools, and the CRL Updater.[2]

1.10 Certificate DN Patterns

DBsign 4.0 has some new parameters which allow applications finer grained control over which users can digitally sign data. In DBsign 3.0, control over who could sign data was limited to the Trusted Certificates list and user-to-certificate mapping with the User

2 In DBsign 4.0, passwords are stored in encrypted format in the configuration file.

Manager administration tool. DBsign 4.0 retains these features but adds a new mechanism called Certificate DN Patterns. Certificate DN Patterns enforce a policy based on information contained in the subject and issuer distinguished name (DN) fields in the user's certificate. Patterns (i.e., “regular expressions”) can be specified that either accept or reject the subject DN or issuer DN fields of users' certificates. For example, only users from the Engineering department can be allowed by specifying that the subject DN must include “ou=Engineering”. Or, all certificates issued by the Accounting department's CA can be excluded by rejecting all certificates that include “cn=Accounting CA”, for example. Since the Certificate DN Patterns are regular expressions, the matching rules are well defined and extremely flexible.

2.0 Backward compatibility

2.1 Support for DBsign Web Signer 3.0

The DBsign Server 4.0 is completely backward compatible with DBsign 3.0's Web Signer control/plug-in client. This means that existing applications can upgrade to the DBsign Server 4.0 without required changes to their application code.

2.2 DBsign Database Structure

DBsign 4.0 requires an update to the database structure of the DBsign System Tables and DBsign Signature Tables. No changes are required to the application's tables and no documents need to be re-signed. All existing digital signatures are preserved. These changes are the result of DBsign 4.0 storing DBsign related dates in the GMT timezone instead of the local database timezone. Storing dates in GMT preserves the true time values if a system changes time zones.