USDM Simplify, Unify, Optimize
Life Science Compliance for Regulated Systems

Oracle WebCenter Content

21 CFR Part 11 Certification

Kim Hutchings
US Data Management
Phone: 888-231-0816
Email: khutchings@usdatamanagement.com

Introduction

In May 2011, US Data Management (USDM) was commissioned to test Oracle's WebCenter Content 11g enterprise content management (ECM) platform to determine its compliance with the U.S. Food and Drug Administration regulation 21 CFR Part 11. This regulation requires that computerized systems include technical controls to assure that electronic records maintain security and integrity and are essentially as inspectable as paper records, and to assure that electronic signatures meet standards that allow them to have the same legal bearing as traditional handwritten signatures.

Summary of Findings

USDM conducted independent Part 11 assessment and testing activities using industry-standard criteria for determining compliance, and found that Oracle WebCenter Content 11g meets the technical requirements of 21 CFR Part 11 and is well-suited for implementation by companies in the life science industries.

The following pages contain the results of Oracle WebCenter Content testing as they pertain to the relevant sections of Part 11.

Electronic Records

11.10 Controls for Closed systems

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine.

Oracle WebCenter Content assures electronic record integrity through robust security and record management services. The Oracle content repository assures that records are automatically identified, secured, versioned, and tracked for changes.

Oracle WebCenter Content protects the confidentiality, integrity, authenticity, availability, and non-repudiation of electronic records and actions taken with electronic records through a variety of means. Authentication is used to uniquely identify users and to indicate who has created, modified, deleted, or signed electronic records. Authorization via user roles and/or granting of granular permissions, combined with access controls applied to libraries and records, allows application administrators and record administrators to grant or deny the ability for users to view, print, create, modify, or delete records.

When a record is stored by the system a secure hashing algorithm creates a message digest unique to the record is created. Any subsequent change to the record will cause a comparison to the stored message digest to fail, indicating a lack of record integrity.

The system audit trail further protects records by logging change activities, and protects against repudiation by logging system activities and identifying the users who performed them.

11.10(a) Validation

Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

Validation of a commercial application for use in a GxP-regulated environment consists of two major areas of focus:

- Activities to assure the design, development and testing performed by the supplier meet regulatory expectations
- Activities to assure that the system as deployed by the user meets regulatory expectations and is suitable for its intended purpose

Oracle addresses the first area of focus by utilizing industry-standard system development lifecycle methodologies, software engineering and quality assurance practices, configuration management practices, and standardized methodologies for development testing, formal acceptance testing, and release management. Oracle also addresses this area of focus by building into Oracle WebCenter Content the technical security and Part 11 controls that are fundamental to successful validation.

Customers who use Oracle's products for GxP purposes are expected to verify Oracle's compliance in these areas. To enable this, Oracle can host a supplier audit where the

customer can inspect and document the sufficiency of Oracle's software design controls. If desired, USDM can assist customers in conducting such audits.

The second area of focus must be addressed by the customer through activities that result in documented specifications and evidence showing, at a minimum:

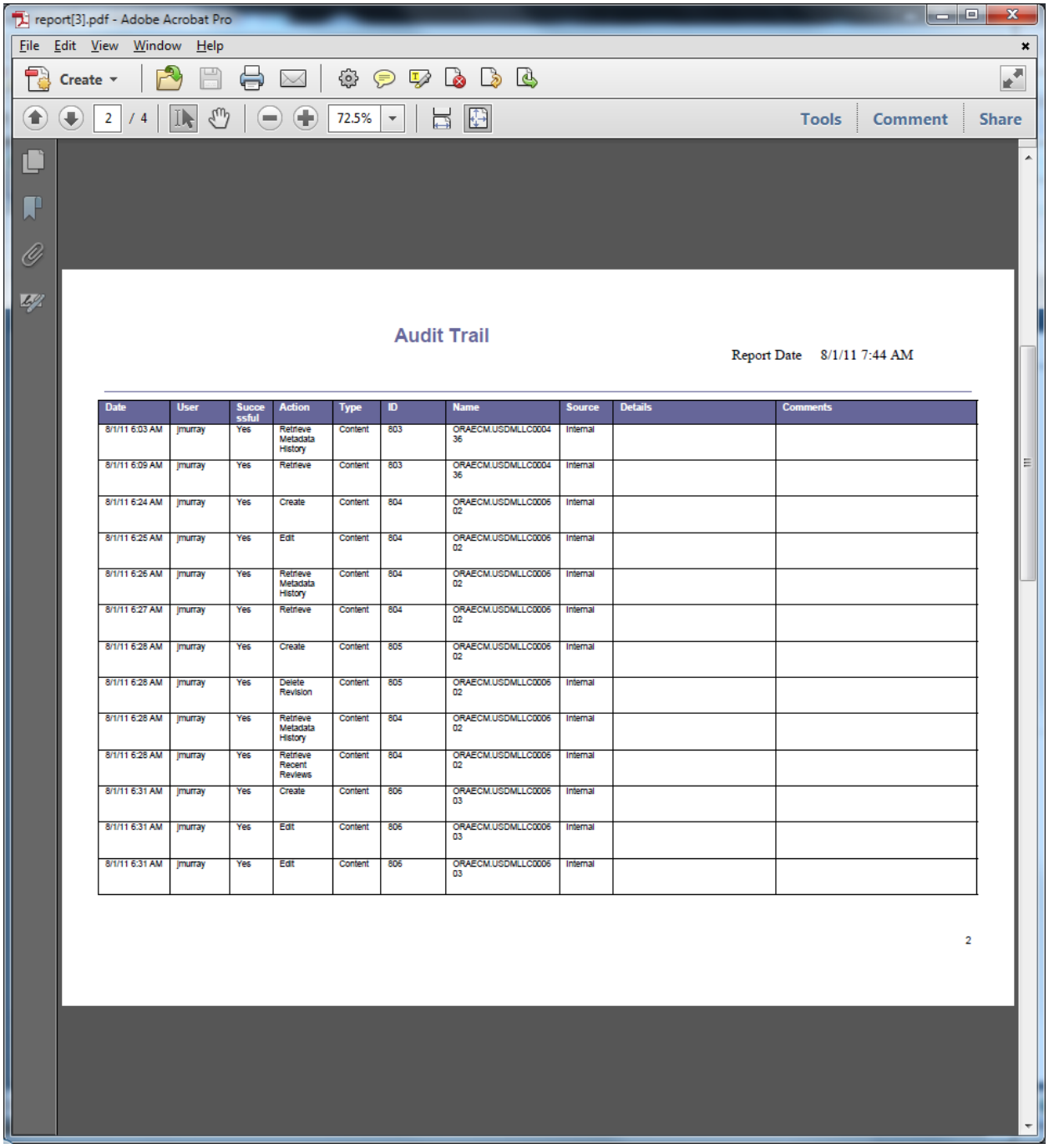
- How the system will be used
- How it will be configured
- How it will be deployed
- That it was installed successfully
- That it functions correctly and properly automates the regulated processes and records

There are industry-standard accepted validation methodologies that Oracle WebCenter Content customers can apply when validating the system. If desired, USDM can help customers to achieve risk-based, GAMP 5-compliant system validation. USDM can lower the cost of validation and reduce the time validation takes by using its Validation Accelerator Pack (VAP) for Oracle WebCenter Content. This VAP contains pre-developed validation specifications and test protocols that need only be customized for the customer's intended use of the system.

11.10 (b) Copies of Records

The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

Inspectors can be allowed view-only access to system records if desired by the customer. In addition, the Oracle WebCenter Content application administrator has the capability of making copies of records in both native and PDF formats.



Date	User	Successful	Action	Type	ID	Name	Source	Details	Comments
8/1/11 6:03 AM	jmurray	Yes	Retrieve Metadata History	Content	803	ORAECM.USDMLLC000436	Internal		
8/1/11 6:09 AM	jmurray	Yes	Retrieve	Content	803	ORAECM.USDMLLC000436	Internal		
8/1/11 6:24 AM	jmurray	Yes	Create	Content	804	ORAECM.USDMLLC000602	Internal		
8/1/11 6:25 AM	jmurray	Yes	Edit	Content	804	ORAECM.USDMLLC000602	Internal		
8/1/11 6:26 AM	jmurray	Yes	Retrieve Metadata History	Content	804	ORAECM.USDMLLC000602	Internal		
8/1/11 6:27 AM	jmurray	Yes	Retrieve	Content	804	ORAECM.USDMLLC000602	Internal		
8/1/11 6:28 AM	jmurray	Yes	Create	Content	805	ORAECM.USDMLLC000602	Internal		
8/1/11 6:28 AM	jmurray	Yes	Delete Revision	Content	805	ORAECM.USDMLLC000602	Internal		
8/1/11 6:28 AM	jmurray	Yes	Retrieve Metadata History	Content	804	ORAECM.USDMLLC000602	Internal		
8/1/11 6:28 AM	jmurray	Yes	Retrieve Recent Reviews	Content	804	ORAECM.USDMLLC000602	Internal		
8/1/11 6:31 AM	jmurray	Yes	Create	Content	806	ORAECM.USDMLLC000603	Internal		
8/1/11 6:31 AM	jmurray	Yes	Edit	Content	806	ORAECM.USDMLLC000603	Internal		
8/1/11 6:31 AM	jmurray	Yes	Edit	Content	806	ORAECM.USDMLLC000603	Internal		

Secure, Accurate Copy of Audit Trail

11.10 (c) Protection of Records

Protection of records to enable their accurate and ready retrieval throughout the records retention period.

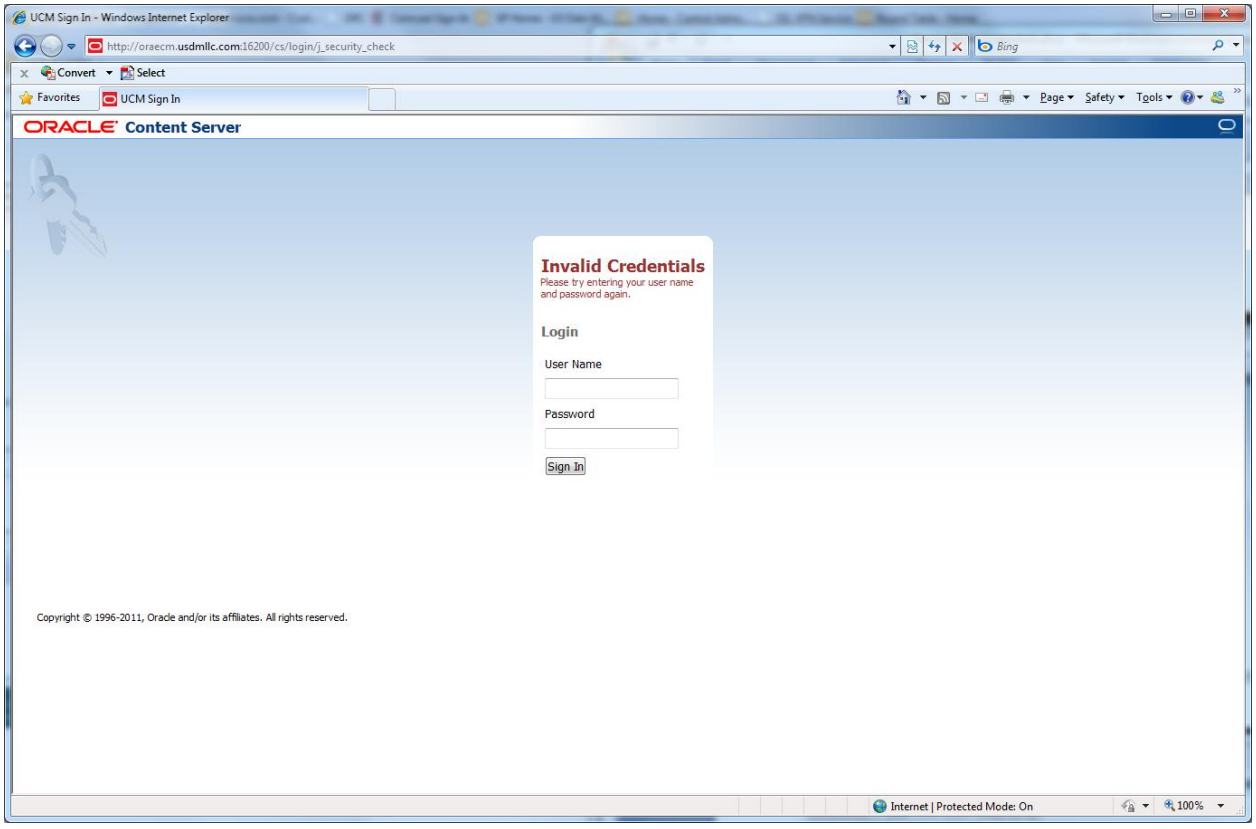
Protection of records is discussed in section 11.10 above. In addition, the metadata for a record can be configured to contain an expiration date that corresponds with the end

of the record's retention period. This can either trigger a defined workflow to disposition the record, or can trigger a notification to the application administrator or record administrator indicating that the record has expired and that manual action is required.

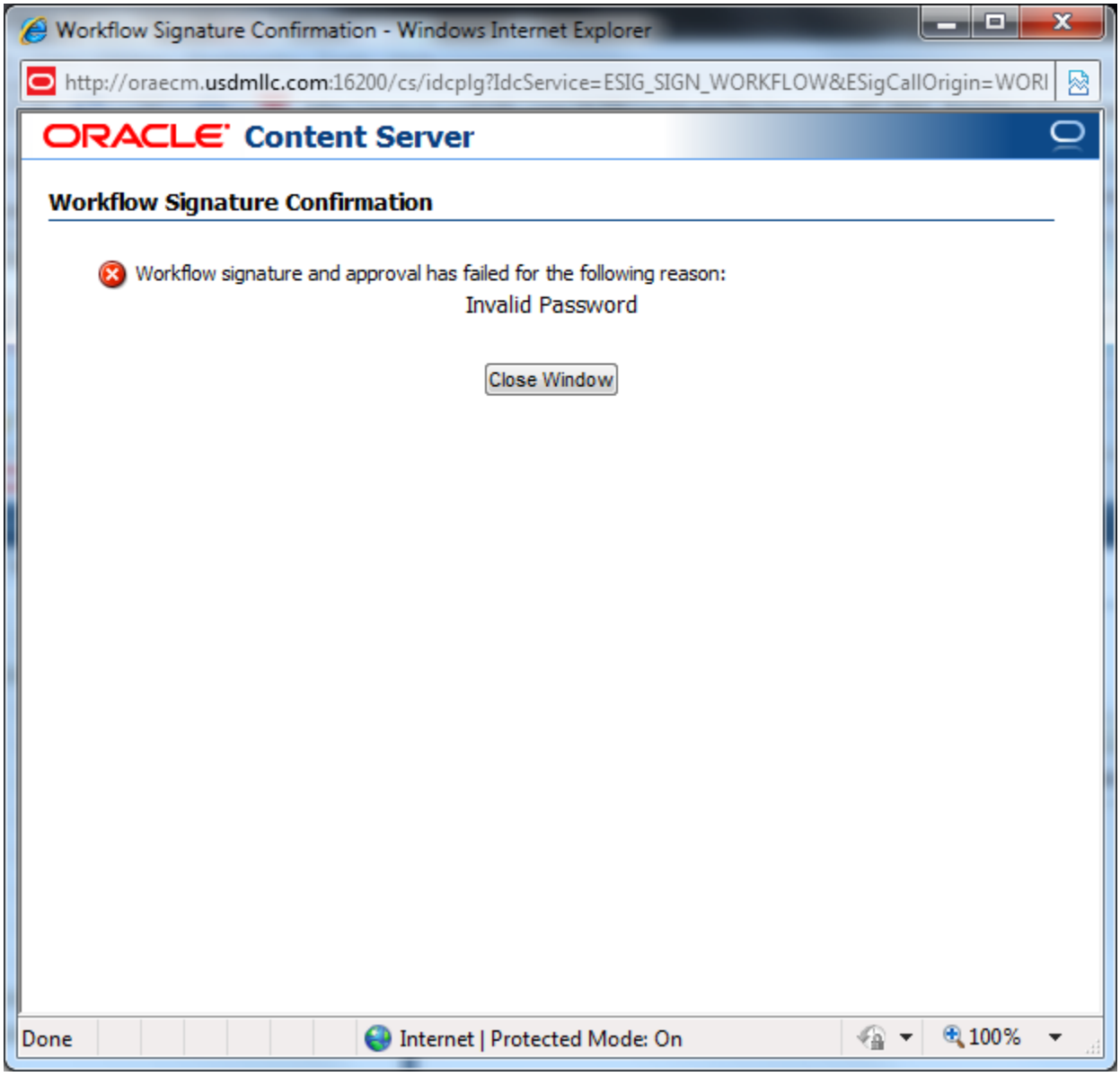
11.10 (d) System Access

Limiting system access to authorized individuals.

This is discussed in general in section 11.10 above. Oracle WebCenter Content limits system access to authorized individuals through user authentication, and limits authorized users to only the approved activities and record access granted to their respective roles. Oracle WebCenter Content authentication integrates seamlessly with server operating system authentication services as well as with network single sign on directory authentication services such as Microsoft Active Directory or Oracle Authentication Services.



Authentication



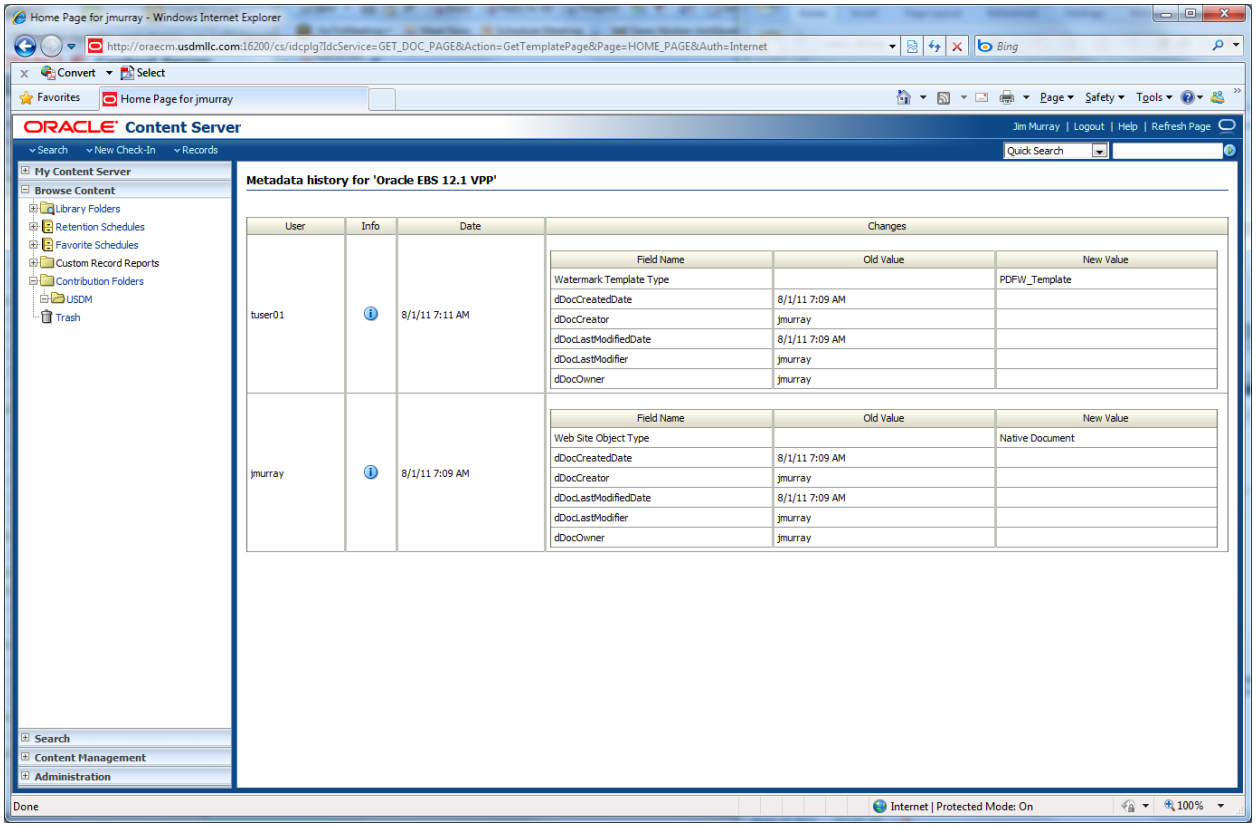
Oracle Signature Authentication

11.10 (e) Audit Trails

Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.

Oracle WebCenter Content is protected by a secure, computer-generated audit trail that records user actions and workflow events. Changes to system records can be traced and the record content prior to the change can be reconstructed. The user ID and the

date and time of the event are captured, and workflow events can be configured to record a reason for the event/change.

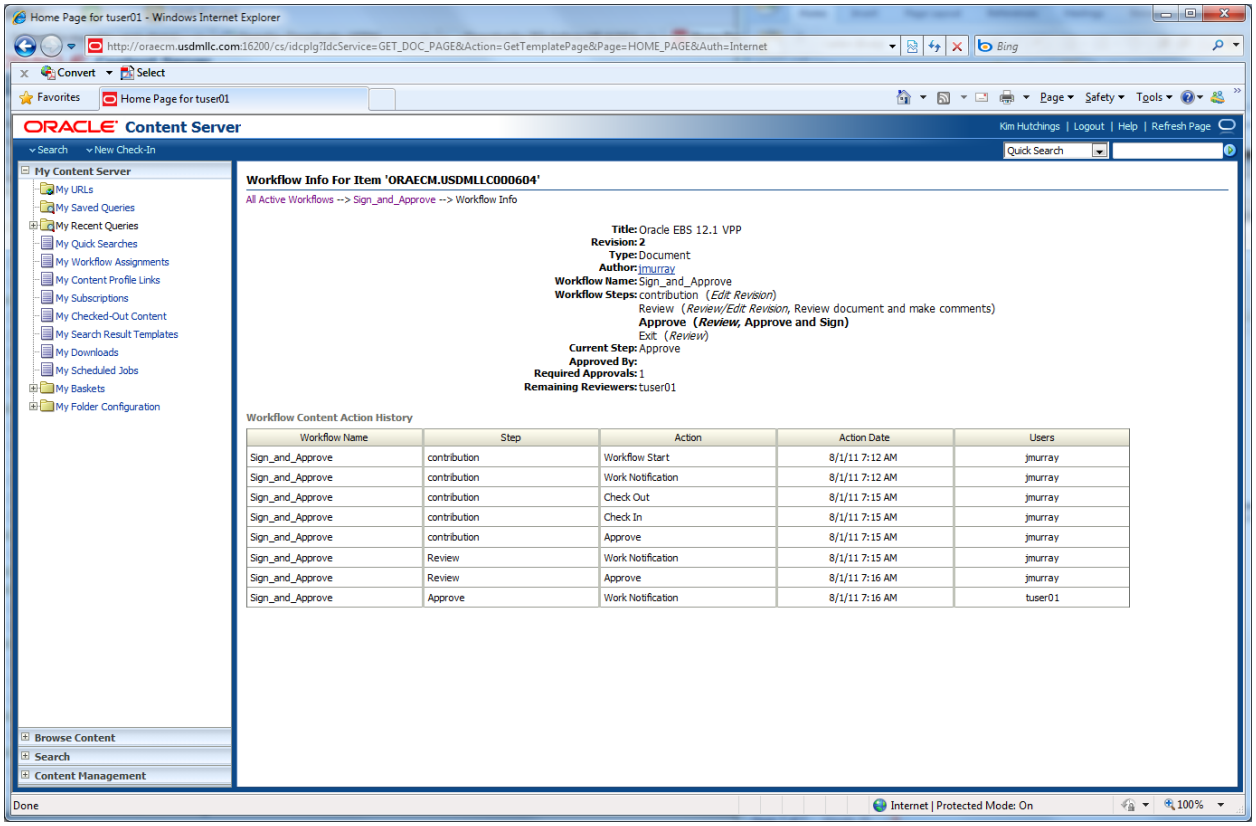


Oracle Metadata Audit Trail

11.10 (f) Sequencing of Events

Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

Oracle WebCenter Content workflows are configurable in a stepwise manner and system users are constrained to execute workflows within the permitted sequence.



Sequencing of Events (Workflow)

11.10 (g) Authority Checks

Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

Records within Oracle WebCenter Content are protected via a highly granular security model. Records are assigned to security groups and optionally to security accounts. Users are assigned permission levels for groups and accounts and are allowed to work with controlled permission levels (Read, Write, Delete, and Administer) only on records and activities for which they possess the appropriate group/account permissions. These permissions can be granted via user roles in a role-based security mode and can be further customized at the user account level.

Further, when Oracle WebCenter Content process workflows are used, workflow steps can be configured such that only individuals with certain roles or permissions can execute the steps.

11.10 (h) Device Checks

Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

Not applicable for this certification. Any workstation may be used to connect to Oracle WebCenter Content (assuming successful authentication of the authorized user).

11.10 (i) Training

Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

Not applicable for this certification. This is a procedural control that must be implemented by the customer. If desired, USDM can help customers implement required Part 11 procedural and administrative controls.

11.10 (j) Electronic Signature Accountability

The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

Not applicable for this certification. This is a procedural control that must be implemented by the customer.

11.10 (k) Control of System Documentation

Use of appropriate controls over systems documentation including:

(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

Not applicable for this certification. This is a procedural control that must be implemented by the customer.

(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

Not applicable for this certification. This is a procedural control that must be implemented by the customer.

11.30 Controls for Open Systems

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in Sec. 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

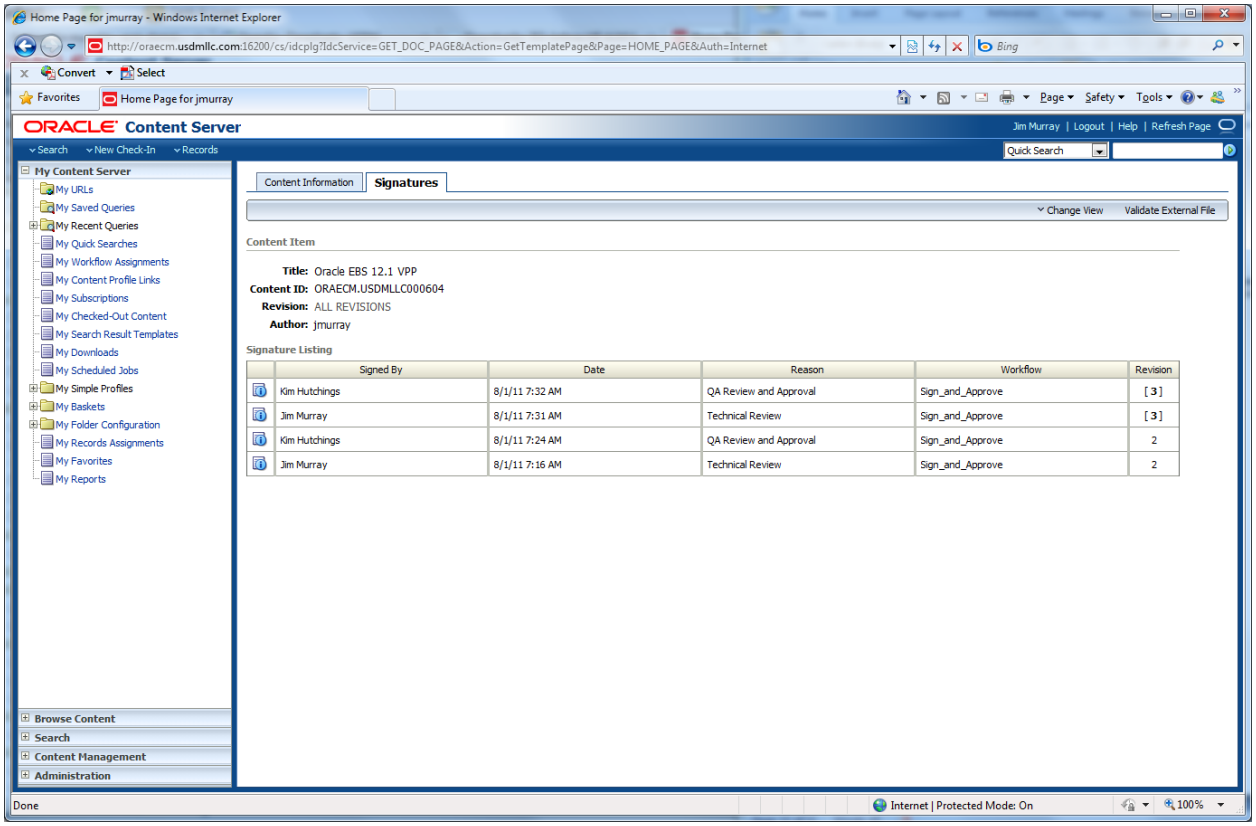
Oracle WebCenter Content supports secure HTTP (HTTPS) and/or Secure Socket Layer (SSL) session encryption to protect sessions and records from unauthorized access. Oracle WebCenter Content can also be accessed via encrypted virtual private network (VPN) links.

Electronic Signatures

11.50 (a) Content of Signature Manifestation

Signed electronic records shall contain information associated with the signing that clearly indicate the printed name of the signer, the date and time when the signature was executed, and the meaning (such as review, approval, responsibility, or authorship) associated with the signature.

Signed records are rendered by the Oracle system as secure PDF versions of the original document. The signature manifestation can be configured to contain the user name, the date and time of the signing, and the reason for (meaning of) the signature. And because the signature is a electronic signature, any changes to the record after the signature is applied can be detected.



Signature Manifestation

11.50 (b) Control and Display of Signature Manifestation

The items identified in 11.50(a) shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

The signature information appears on both electronic and printed versions of the signed rendered PDF document.

11.70 Signature/Record Linking

Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

Oracle WebCenter Content electronic signatures are linked to their signed records in three ways.

- The record metadata contains the current status of all versions of the records it manages, including whether a record has been signed/approved and by whom.
- Oracle WebCenter Content allows publishing of a rendered PDF version of the record which contains the manifestation of the electronic signature, which in turn allows signed records used outside of the Oracle system to maintain the signature/record link.
- Oracle WebCenter Content maintains an audit trail which indicates that the signature occurred, the user ID of the signer, and the date and time the signature was applied to the record.

11.100 General Requirements

11.100 (a) Uniqueness of Signatures

Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

The key to assuring the uniqueness of an electronic signature is to assure that the user identification code is unique. Oracle WebCenter Content and authentication services such as Microsoft Active Directory and Oracle Authentication Services all enforce this rule. Given uniqueness of the user identification, both the electronic signature execution/signing (which uses the user identification as an authentication credential) and the electronic signature manifestation (which includes the user identification) are guaranteed to be unique.

11.100 (b) Identification of Signers

Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.

Not applicable for this certification. This is a procedural control that must be implemented by the customer.

11.100 (c) Equivalence to Handwritten Signatures

Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

Not applicable for this certification. This is a procedural control that must be implemented by the customer.

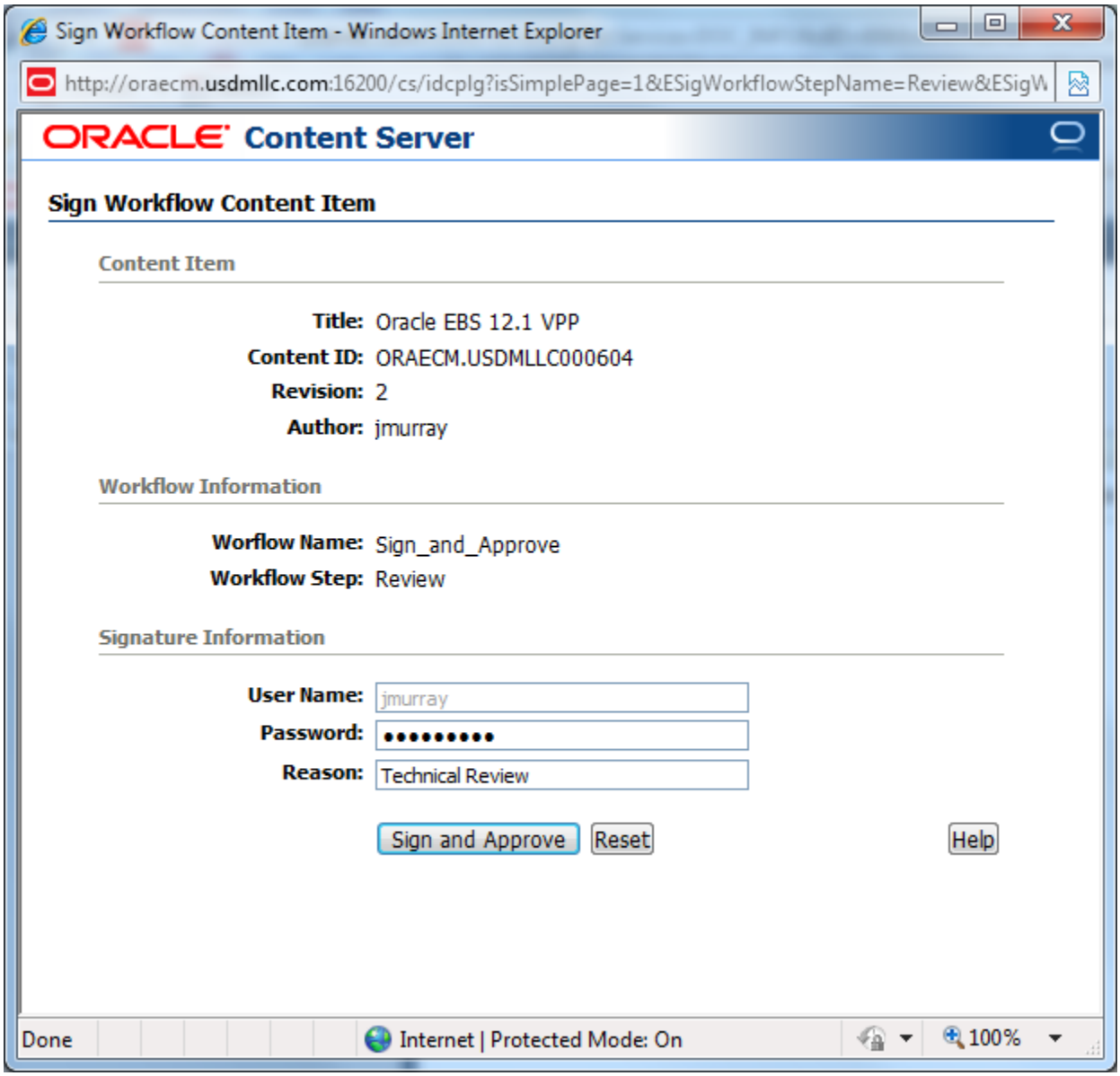
11.200 Electronic Signature Components and Controls

11.200 (a) Non-Biometric Signatures

Electronic signatures that are not based upon biometrics shall employ at least two distinct identification components such as an identification code and password, shall be used only by their genuine owners, and shall be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

The combination of operating system security and Oracle WebCenter Content security ensure this. Both user identification code and password are required to authenticate during system login and during electronic signature executions. Passwords are protected such that anyone other than the genuine owner would need to collaborate with either the original owner or the application/network administrator.

Note: The operating system protects against tactics such as "brute force" attempts at unauthorized password use (something the authors of Part 11 did not consider) by reporting these and disabling accounts after multiple unsuccessful attempts.

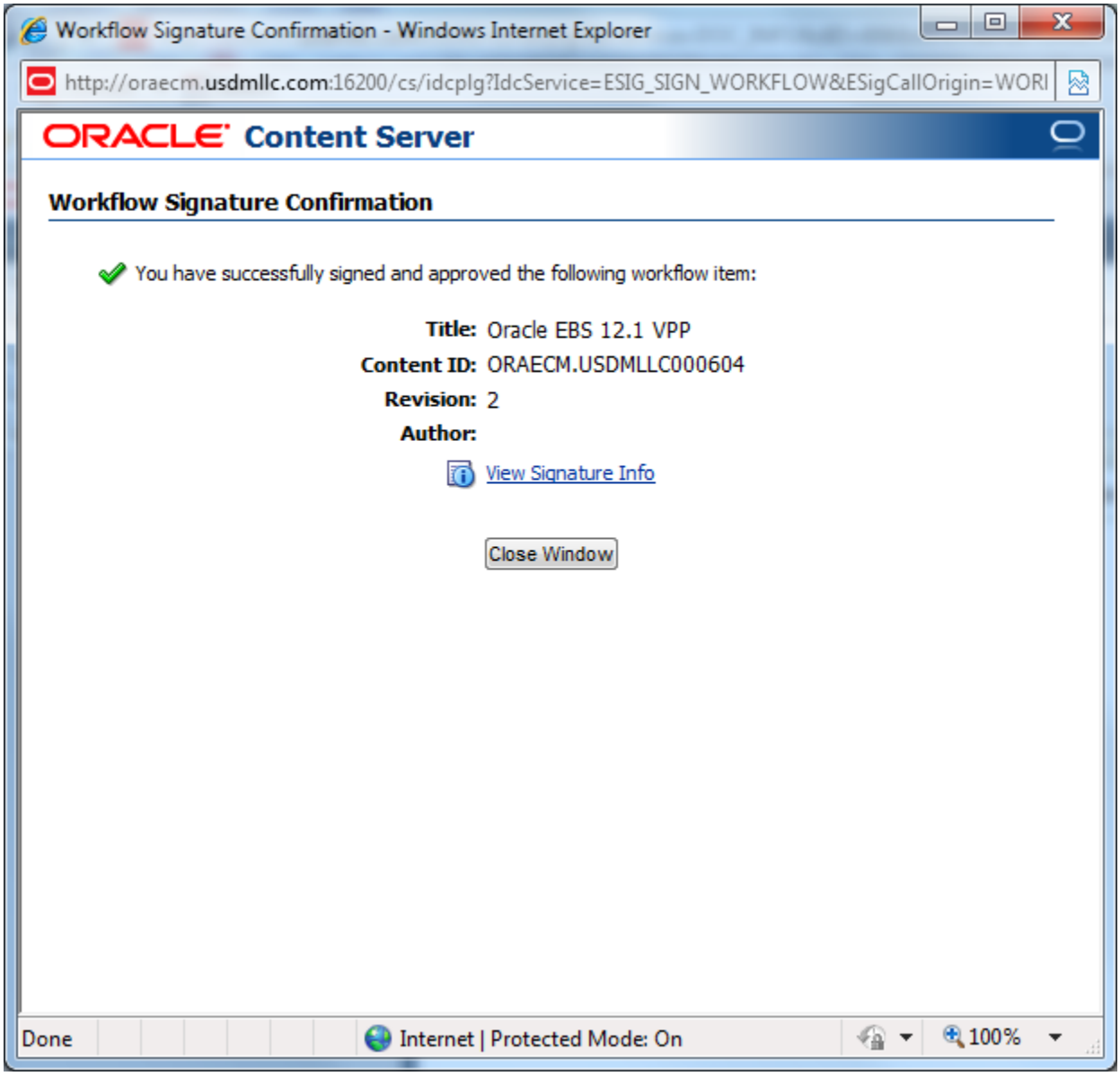


Oracle Signature Authentication

11.200 (a)(1) Series of Non-Biometric Signings

When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

Oracle WebCenter Content requires the use of both user identification code and password when executing electronic signatures.



Oracle Signature Authentication

11.200 (b) Biometric Signatures

Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

Not applicable for this certification. This involves technical and procedural controls that must be implemented by the customer.

11.300 Controls for Identification Codes/Passwords

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity.

As discussed previously, the combination of Oracle WebCenter Content and operating system security provide technical protection of passwords to prevent their unauthorized use.

For complete password integrity, the user must also implement procedural controls (e.g. that users not share passwords with others).

11.300 (a) Uniqueness of Identification Code/Password

Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

As discussed in section 11.100(a) above, the key to meeting this requirement is to enforce uniqueness of user identification codes. Both Oracle WebCenter Content and external authentication services enforce the rule that no two user accounts have the same user identification code.

11.300 (b) Password Management

Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

The combination of Oracle WebCenter Content and external authentication services can be configured to enforce password aging, password strength rules, required password changes upon first login, etc.

Meeting this requirement completely also requires a procedural control that must be implemented by the customer.

11.300 (c) Device Loss Management

Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.

Not applicable for this certification. This involves technical and procedural controls that must be implemented by the customer.

11.300 (d) Transaction Safeguards

Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

The combination of the network operating system (if external authentication is used) and Oracle WebCenter Content will detect and report the unsuccessful use of authentication credentials for system login attempts and electronic signature execution attempts.

This also requires a procedural control that must be implemented by the customer.

11.300 (e) Device Testing

Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

Not applicable for this certification. This is a procedural control that must be implemented by the customer.

This whitepaper is available on the USDM website:
http://usdatamanagement.com/validation-accelerator-packs-for-ecm-systems/175-validation-package-for-oracle-content-management.html

Additional information about the Oracle WebCenter Content platform can be found at www.oracle.com/goto/ecm .