Appendix E Security solution implemented within database-driven GIS Web portals & Web maps

The encryption solution can be used for protection of spatial files within a database-centric Web Portal. When GIS users first access the Portal, they see only the public pages and content. To see the protected GIS content, they must be authenticated as one of the authorized Portal user or administrators. Furthermore, the encryption model for files stored in Oracle Portal is similar to our encryption solution for DBFS using ECMSDK, with slight modifications to the procedures, since both products store file content and metadata within the database.

E.1 Single-user and multi-user spatial file encryption schemes

In contrast to ECMSDK, Oracle Portal stores the document metadata and content in the same table; in the **WWDOC_DOCUMENT$**. Thus, information on user-owned sensitive spatial files were retrieved from the same table. The only distinction to the above procedures was the Portal schema, table, and column names in the cursor definition statement. Code segment attached below generates the list of Portal single-user files that have an ***_enc*** file suffix from the Portal schema tables. The ids of these files can then be passed to the encryption and decryption script one by one for encryption and decryption respectively.

```
CURSOR portal_user_files IS
   SELECT name, id FROM PORTAL30.WWDOC_DOCUMENT$ WHERE creator = v_userid
   AND (name LIKE ‘%_enc’);
```

For sensitive files requiring project level multi-user access, the encryption scheme prepared for ECMSDK users can be developed with slight modification to the content and metadata tables.

E.2 Automated decryption and encryption

Implementation of an automated decryption and encryption model for sensitive files in Portal can be based on Portal user session table **WWCTX_SSO_SESSION\$** within the **PORTAL30** schema table which call the decryption and encryption procedures passing the Portal **user id** from the ID column

However, these sensitive files can be vulnerable when Portal users do not log out properly by shutting down the browser instead of clicking the logout link. In this case, the Portal user session will still be active, and the decrypted files would not be encrypted back for protection. To resolve this, a session cleanup procedure provided by Oracle 9i Portal can be used, namely **ctxjsub**, which can be run periodically as a DBMS job to perform session cleanup for the Portal session table **WWCTX_SSO_SESSION$**. This would delete all inactive sessions, and subsequently the triggers will be fired which would call the encryption procedures to encrypt files back for protection.

An absolute security approach for the GIS Portal could require encryption of Web Mapping files as well. The following section describes how the Web maps personal geodatabase flat files can be encrypted within in Portal as well as.

E.3 Encryption of WebMap geodatabase files

The flat files geodatabases within Web Map applications can be stored and protected within a DBFS. For instance, WebMap geodatabases in Ms Access format can be protected with Oracle ECMSDK folder and file ACL security. Thereafter, these files can be protected against storage media compromise via encryption and decrypted only for use.

The personal geodatabases can be protected using the multi-user access encryption scheme. The end-users would login credentials would be authenticated against those for ECMSDK that will be retrieved from Portal SSO servers and OID. Subsequently, the ECMSDK user sessions triggers would decrypt the files for use and encrypt back for protection when the user session(s) terminate with the logout link.

Figure 17 illustrates the Oracle Portal security model. When users first access the Portal, they only see the public pages and content. To see the protected GIS content, they must be authenticated as an authorized Portal user. The Portal first provides SSO page for users to enter credentials for authentication, which are encrypted in-transit. Upon successful authentication and subsequent Portal user session creation, project-specific and single-user Portal files are decrypted for use.

Thereafter, end-user actions on Portal are controlled through page, content area, folder, and item level ACL security. These are enforced regardless of whether users access through the page interface or directly through the content area. Requests for Web Mapping services are directed to Portal external application provider that authenticates users against their accounts in the Web Map server on their behalf after retrieving them from the OID, providing single sign-on for Web Map external application. After user has finished working with the Portal and logging out successfully, the files would be encrypted back for secure storage.

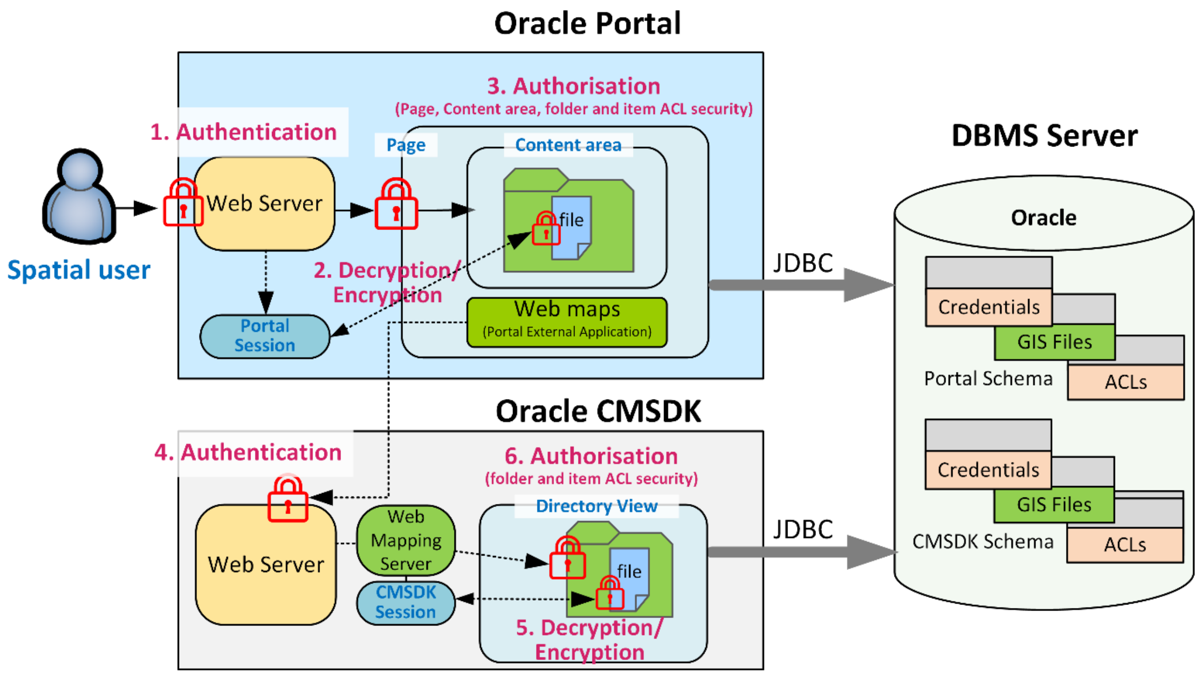

Figure 17: User interaction model for the proposed storage security solution implemented for spatial files within a database-centric web portal and for geodatabases in Web mapping service. Sensitive spatial files are automatically decrypted for use and encrypted back after use.

Security principles to authenticate and authorize users for accessing the protected GIS content through Oracle Portal are as follows:

1. The Portal HTTP Server displays the users with Single Sign-On (SSO) login page for submitting their SSO username and password; this will be the only set of credentials they will have to provide; which are protected in-transit using Portal SSL encryption.

2. The SSO Server verifies the credentials against those stored in OID. If the authentication is successful, the SSO Server creates a session cookie for the user. Information within this session cookie is later used to query the user’s privileges specified in OID.

3. Only authorized Portal users can have access to the protected content within the Portal.

4. Portal user-session creation will fire the session-based trigger, calling the decryption procedure upon which the project-specific and single-user files will be decrypted for use.

5. Portal page ACL security controls access to pages; the first part of the Portal authorization process. From within these pages, requests for accessing protected GIS content, are directed to the associated category through the respective portlet.

6. All actions on content are controlled at multiple levels: Portal content area, folder, and item ACL security. Categories are used to display the list of items associated with that category at the same time preventing direct user access to folders and its content.

7. Folder and item ACL security is used to control permissions on submission folders and content.

8. User request for Web Map is passed to Portal external application provider.

9. The external application provider requests the Single Sign-On server (SSO) for user's credentials in the Web Map Server (WMS). SSO retrieves this from Oracle Internet Directory and returns it to the application provider.

10. The external application provider authenticates users against their accounts in the WMS on their behalf, providing single sign-on for Web Mapping services.

11. When Portal user logs out, the user-session termination fires the session-based trigger which calls the encryption procedure for encryption of the project-specific and single-user files back for secure storage.