LandXML

LandXML – Signing & Sealing

by

Warren G. Clary, PE

LandXML

Can a zipped LandXML file be created whose contents can be signed and sealed? Yes, if some conditions are addressed.

From my experiences at FL DOT, I will present background information and my conclusions on why I think the answer is YES.

Overview

- Electronic Signing & Sealing FL DOT
- LandXML Signing & Sealing
- LandXML File Management
- LandXML Archiving

Electronic Signing/Sealing FL DOT

- Professionals' Electronic Data Delivery System(PEDDS)
  - Process
  - Goals
  - Standards
- Florida Board of Professional Regulation
  - Requirements
  - 1998 Florida Board of Professional Engineering rules
  - Today, Digital Signature PKI
- PEDDS Database
  - Project Archiving
  - Long Term Archiving

PEDDS Process

PEDDS relies on a one-way cryptographic hash function to uniquely identify electronic data, and the hash codes created are protected by the traditional means of manually signing and sealing a paper document.

(That's it.)

PEDDS Process

PEDDS Process:

- **One-way Cryptographic Hash Algorithm**
- **Hash Code**
- **Traditional Signature and Seal**

PEDDS Process

One-Way Cryptographic Hash Functions:

- The hash code is solely dependent on the file's content and the cryptographic hash function
- Easy to generate in one direction - from an input file to the hash code, but hard to go backwards, from a hash code to find a matching input file.

PEDDS Process

Secure Hash Algorithm

- Federal Information Processing Standards Publication 180-1 (FIPS Pub 180-1)
- Adopted by the US Government in 1995

PEDDS Process

How Secure in Today's Technology:

Given a file and its Hash Code, how difficult to find another file with the same Hash Code?

- Given 1 million dollars for a computer
- You would have a 50/50 chance of finding another file with that hash code in 100,000,000,000 years.

PEDDS Process

File’s Electronic Signature:

- SHA-1 creates a unique 160-bit message Digest (or Hash Code) for each input file.
- No files with different content will create the same Hash Code.
- If the file's content is unchanged it will always produce the same Hash Code.
- You intend to use the Hash Code to identify the file.

PEDDS Process

SHA-1 Hash Codes
As
Hexadecimal Numbers

E059A970-E74332B9-C88EFE6B-07AEF50B-8DAD3F1E

C67AA18D-BB796868-864D6012-20303B8B-07CC4600

PEDDS Process

- Compute a file’s Hash Code
- Use the Hash Code as an electronic signature
- Print the Hash Code in Hexadecimal Format
- Associate the Hash Code to one signature
- Sign the printed document

PEDDS Process

Print and sign this document

The hash code listed below is used as an electronic signature to affix the undersigned signature to the electronic file which has this hash code.

File name: ./contract.txt

SHA-1 Hash Code:
46C8CAA3-85044917-A6FAA923-A1DA825A-7885C785

My signature would go here_____Date_____
Warren Clary, P.E. - Project Manager

PEDDS Goals

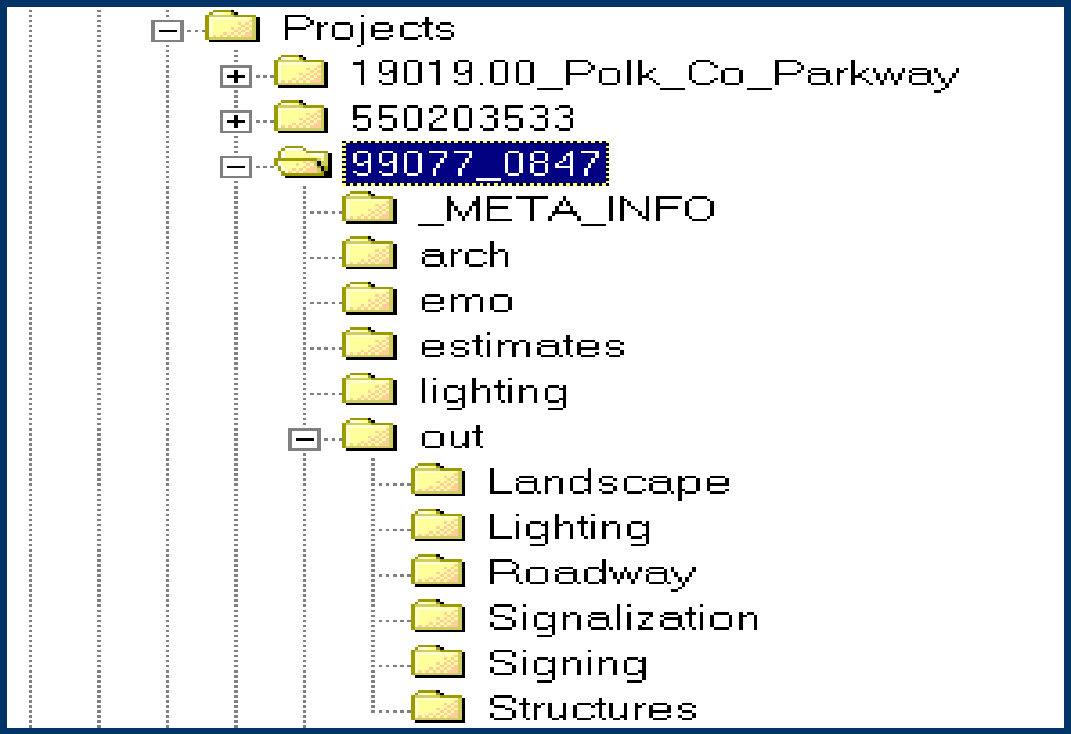
Provide a way to manage electronic data that meets the Department's legal requirements of signing, or signing and sealing, documents in Florida.

PEDDS Goals

Electronic Delivery?

- A set of files under a project directory that define all the project's supporting data used to create the signed and sealed files, and the signed and sealed files themselves.
- Manifest file, signature files, and project identification file.
- The signed and sealed paper documents used to secure the project and sign and seal the files within the project.

PEDDS Goals



Project Dir: D:/Projects/990077_0847
Relative URL: ./_META_INFO/
Relative URL: ./Out/Landscape/

PEDDS Goals

Provide a process whereby:

- A professional engineer or surveyor can sign and seal selected files within the project
- All electronic files in a delivery can be signed
- Signed and sealed electronic files can be authenticated
- A file can have multiple signatures
- All signed electronic files can be authenticated

PEDDS Goals

Authenticate a project:

- Signed, or signed and sealed files are missing
- Signed, or signed and sealed file names have been changed
- Signed, or signed and sealed files have been modified
- Unauthorized files have been added to the delivery

PEDDS Goals

PEDDS Files:

- Manifest file
  - Define the purpose of the delivery
  - Secure the project
    - Project files
    - Signature files
- Signature file
  - Identifies a Professional engineer
  - Defines the purpose of signing or signing/sealing
  - Secures the Electronic Signatures of the signed files
- Project Identification file
  - Created by the Department to identify the project
  - IS NOT SECURED by the Manifest file

PEDDS Goals

Signing and Sealing Engineering Plans:

- Engineers regulated in Florida by Board of Professional Engineers.
- Board adopts rules that govern engineering, including sealing requirements.

PEDDS Standards

- FIPS Pub 180-1 Secure Hash Standard
- Internet Engineering Task Force's Relative URL (RFC 1738)
- World Wide Web Consortium's Extensible Markup Language (XML)

FL Brd. of Professional Regulation

Signing and Sealing Engineering Plans:

- Board rules required the use of an impression type metal seal, then….

1998:

- **Board approves use of hash codes to represent electronic files!**
- **Expands rule for signing and sealing electronic files.**

FL Brd. of Professional Regulation

1998 Florida Board of Professional Engineering rules:

(1) Information stored in electronic files representing plans, specifications, plats, reports, or other documents which must be sealed under the provisions of Chapter 471, F.S., shall be signed, dated and sealed by the professional engineer in responsible charge.

FL Brd. of Professional Regulation

1998 Florida Board of Professional Engineering rules:

(2) Electronic files may be signed and sealed by creating a "signature" file that contains the engineer’s name and PE number, a brief overall description of the engineering documents, and a list of the electronic files to be sealed.

FL Brd. of Professional Regulation

1998 Florida Board of Professional Engineering rules:

Each file in the list shall be identified by its file name utilizing relative Uniform Resource Locators (URL) syntax ….

FL Brd. of Professional Regulation

1998 Florida Board of Professional Engineering rules:

Each file shall have an authentication code defined as an SHA-1 message digest described in Federal Information Processing Standard Publication 180-1 “Secure Hash Standard,” ….

FL Brd. of Professional Regulation

Digital Signature:

A report shall be created that contains the engineer’s name and PE number, a brief overall description of the engineering documents in question and the authentication code of the signature file. This report shall be printed and manually signed, dated, and sealed by the professional engineer in responsible charge.

FL Brd. of Professional Regulation

1998 Florida Board of Professional Engineering rules:

Each file shall have an authentication code defined as an SHA-1 message digest described in Federal Information Processing Standard Publication 180-1 “Secure Hash Standard,” ….

FL Brd. of Professional Regulation

1G15-23.003 Procedures for Signing and Sealing:

(2) A professional engineer utilizing a digital signature to seal engineering work shall have their identity authenticated by a certification authority and shall assure that the digital signature is:

(a) Unique to the person using it;

(b) Capable of verification;

(c) Under the sole control of the person using it;

(d) Linked to a document in such a manner that the electronic signature is invalidated if any data in the document are changed.

FL Brd. of Professional Regulation

Public Key Infrastructure (PKI)

- PKI uses a public key and a private key to secure documents.
- A Certificate Authority is used to:
  - Establish identity
  - Create the public/private key pair
  - Hold the public key where it can be trusted
  - Manage key revocation
  - Time Stamp the period the key can be used
- If the private key is compromised, the key pair needs to be revoked
- Digital Signatures can be either attached or detached from the document
- Attached Digital Signatures modify the file and change its hash code

This can replace the signed and sealed paper document used in PEDDS to secure a signature file.

PEDDS Database

Project Archiving:

- Authenticate project before archiving
- Index projects by ProjectID metadata
- Archive projects
  - Project ID file
  - Manifest file
  - All Signature files
  - Project data files
- All files are stored & named by their SHA-1 code
- The manifest links files SHA-1 to files URL

PEDDS Database

Project Archiving:

- Projects are located by ProjectID metadata
- SHA-1 can be used to locate a single file and determine which project or projects it exists in
- Exported projects are built using
  - Project ID file
  - Manifest file
  - All Signature files
  - Project data files

PEDDS Database

Long Term Archiving:

- The project files are stored outside the Database
- The Database links to the project files using the PEDDS files
- If the Database gets corrupted it can be completely rebuilt from the project files
- The project files and database are backed-up on a regular basis

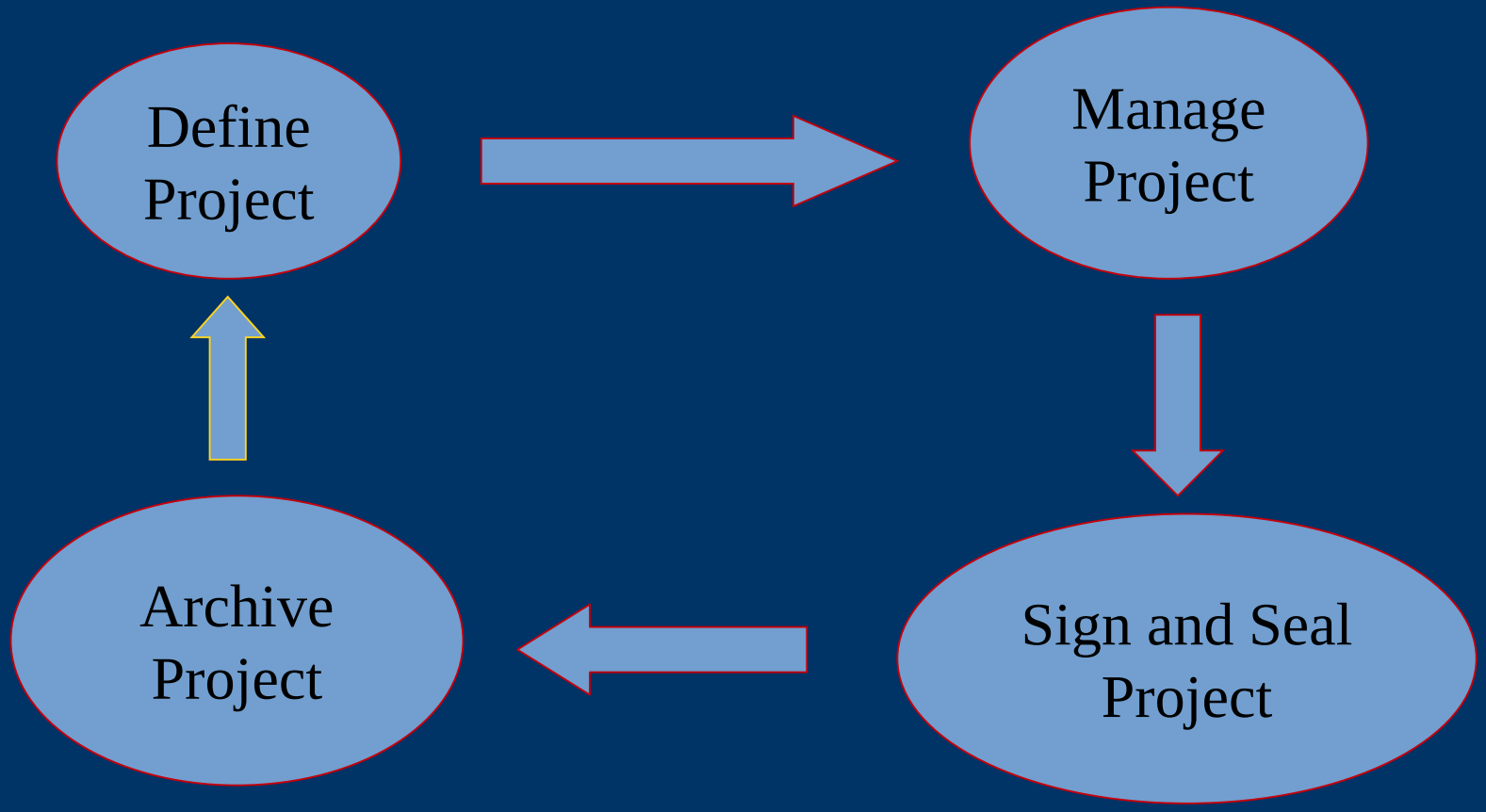
PEDDS Database

Long Term Archiving:

- A Crawler program authenticates the archived files on a regular basis
- This program runs at night when there is idle CPU time, it gets a low priority
- It works it way through the list of stored SHA-1 codes
- It locates the file by its SHA-1 code name, computes the file's SHA-1 code, and compares it to the stored SHA-1 code.
- If there is a mismatch, it is logged and a mismatch alert is sent.

LandXML

Work Flow:



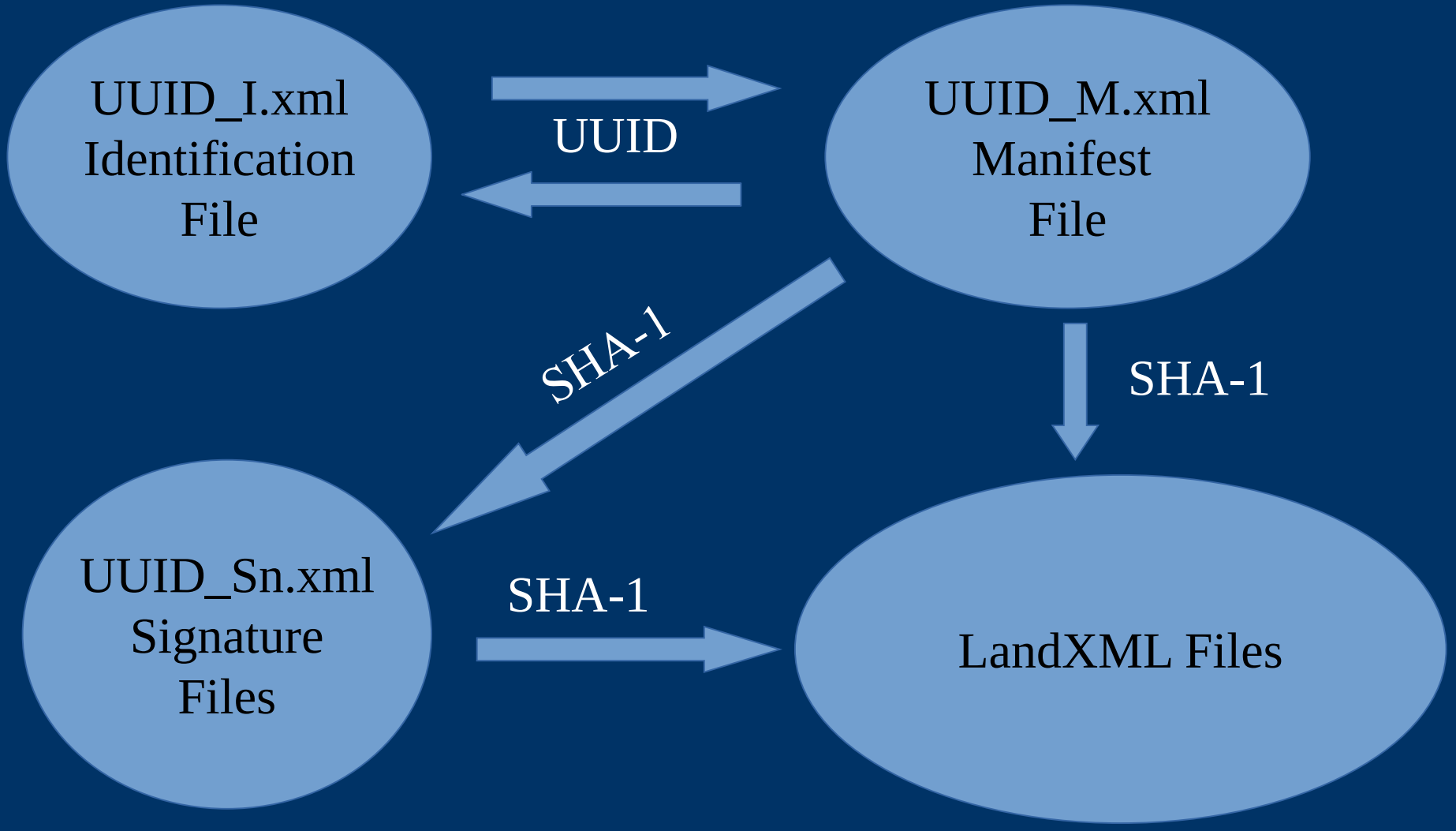
LandXML

Define Project:

- Name - Universal User Identification (UUID)
- Identification file - Metadata
- Manifest file
- Signature files
- Directory structure
- Properties of a zip file

LandXML – Define Project

Project Definition Files:



LandXML – Define Project

Identification file (UUID_I.xml):

- UUID Date Time
- DOT Contract Management Information
- General description
- Plans Components
- Engineer of Record
- Engineers Signing and Sealing
- Location by:
  - District, County, City, Zip code
  - State road numbers, mileposts
  - Geographic point (state plane)
  - Bounded region (state plane)

LandXML – Define Proejct

Manifest file (UUID_M.xml):

- UUID Date Time
- Purpose of delivery
- Signatory who signs the delivery (not sign and seal)
- Signatory's Title
- List of Signature files
  - Relative URLs
  - Hash-codes SHA-1
- List of LandXML files
  - Relative URLs
  - Hash-codes SHA-1

LandXML – Define Project

Properties of a zip file:

- You can archive all the files under a parent directory
- The zip file will have the name of the parent directory with a .zip extension
- If the parent directory name is unique, it can be moved anywhere without conflict.
- The zip file maintains the directory structure and file names
- Even after the zip file is moved, relative URLs within the zip file are valid

LandXML - Define Project

Directory Structure:

- The parent directory of the zip file is much like the root directory in a PEDDS project.
- All the project files are under this directory, but it is not part of the zip file.
- This insures the project can be moved anywhere without conflict.
- The zip file name should reflect the project identification
- A ./meta_info directory will contain the files that define the project

LandXML File Management

File management here refers to how the files are going the be shared and managed during the development of the project.

File Management:

- Maintain local copy
- Save changes locally, with audit trail
- Attach personal identity to changes
- Upload commits to central system
- Resolve conflicts, if any exist, before upload
- Be able to look at difference between changes

LandXML File Management

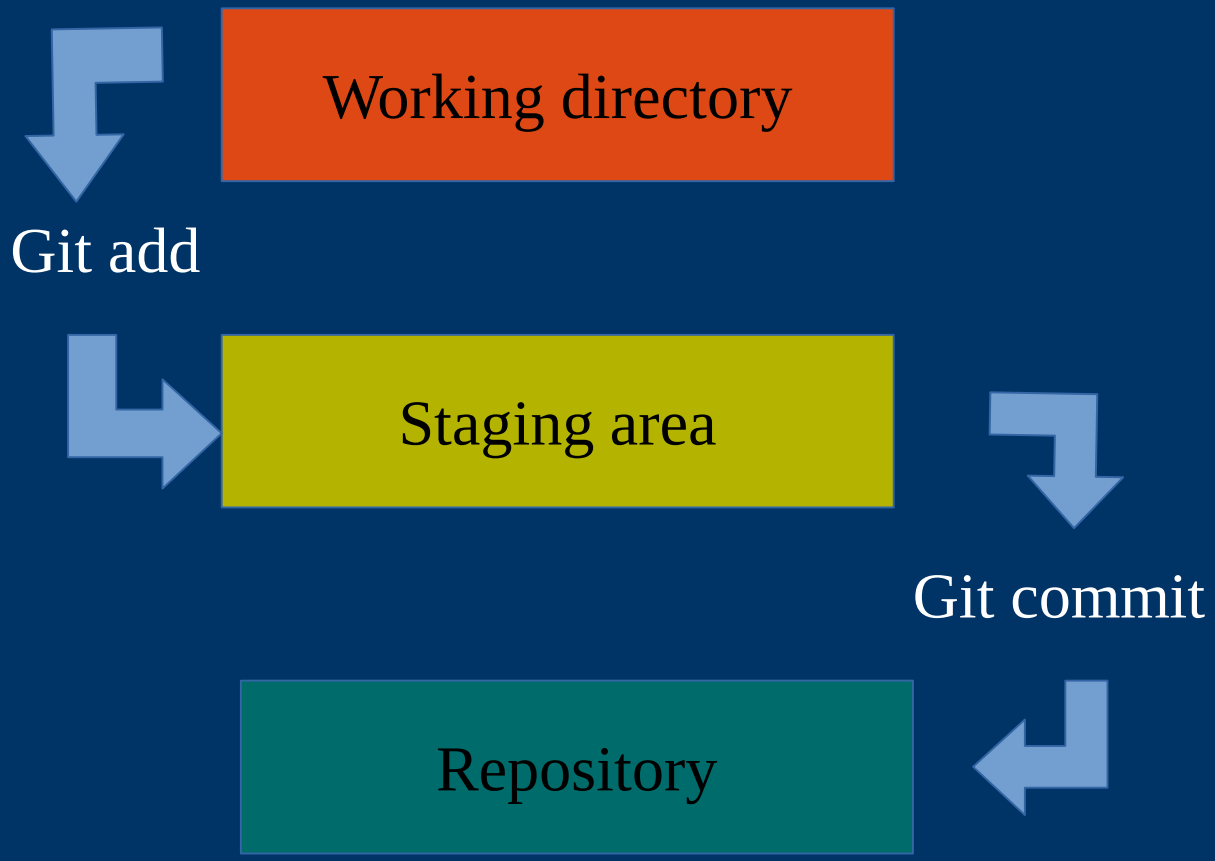
Git is a file management system:

- That maintains your projects locally
- Lets you commit changes to your local system
- You can review the differences between commits
- The older commits only store the differential changes
- The last commit is the full document
- Upload to Git Server for group collaboration

Git home page – http://git-scm.com/
Pro Git Book online – http://git-scm.com/book

LandXML File Management

Git File Management:



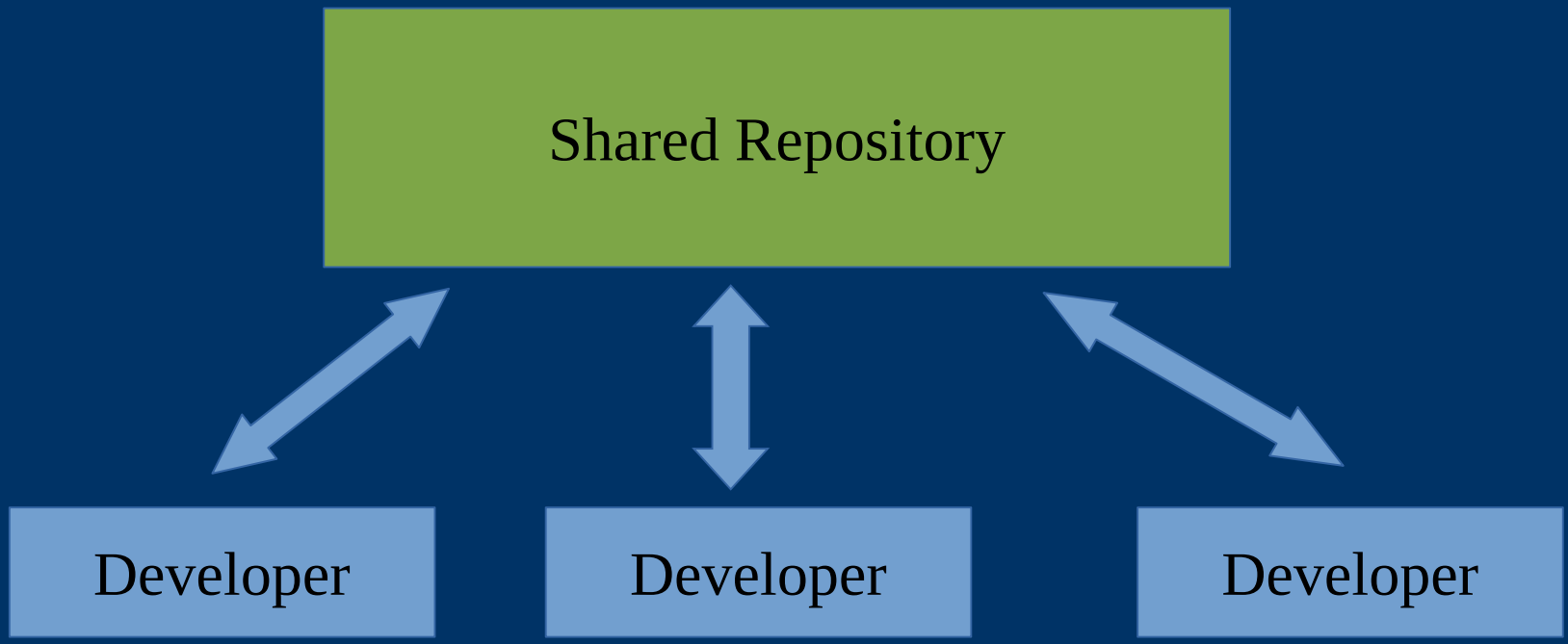
LandXML File Management

Git Server version of Git. This provides the networking capabilities needed to manage projects between groups and multiple locations

Both Git and Git Server have APIs where the software can be customized. Both custom Graphical User Interfaces (GUI) and custom procedures can be developed

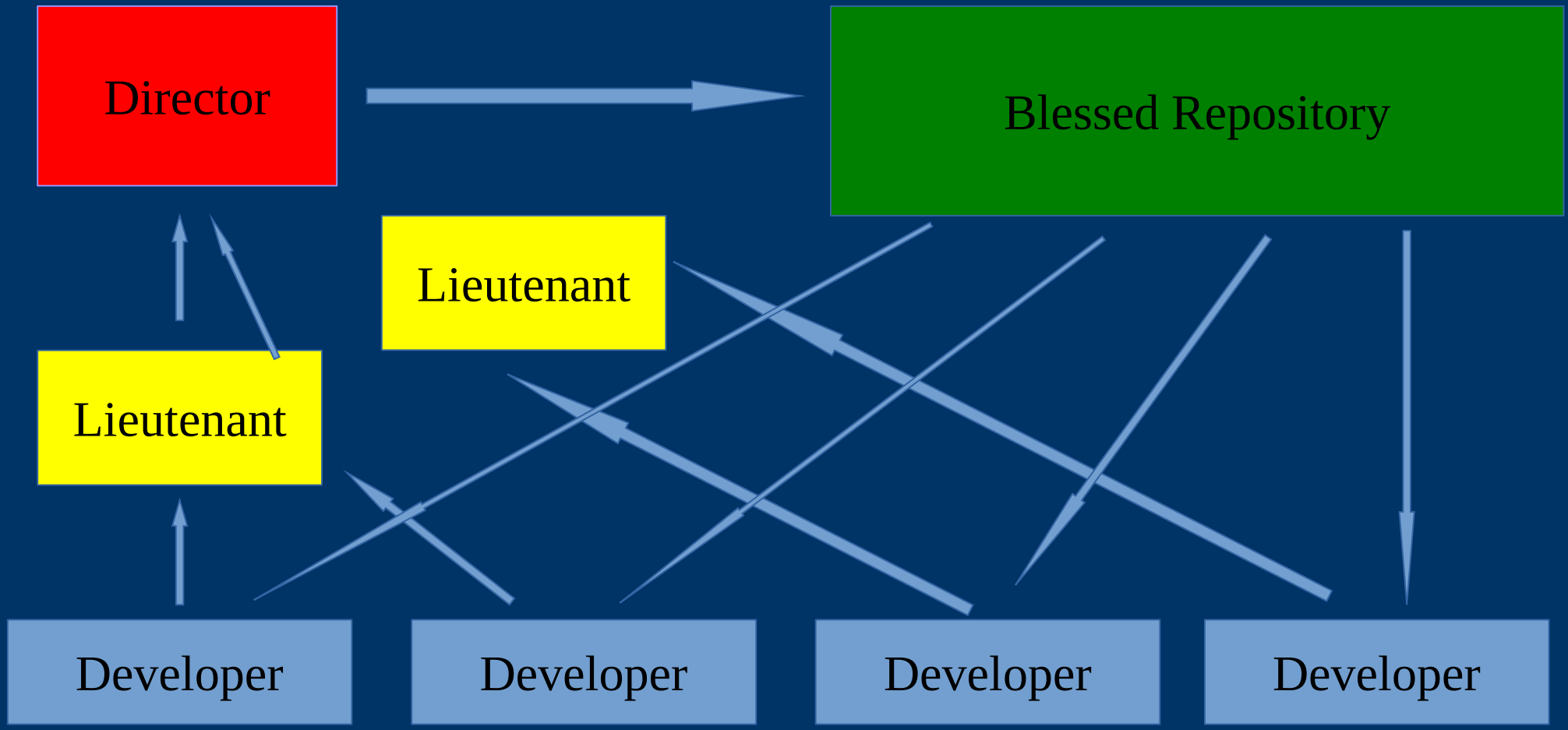
LandXML File Management

Git Shared Repository:



LandXML File Management

Git Director and Lieutenants Workflow:



LandXML Signing and Sealing

Signing and Sealing:

- One signs and seals a file by its hash-code (SHA-1 for example)
- If a Digital Signature is used, it should be detached from the file. If multiple signatures are needed, they will be signing the same hash-code.
- The Digital Signature MUST be stored in the XML Signature Syntax and Processing Version 2.0 as defined by the W3C.
- The Digital Signature can be attached to the signature file

LandXML Signing and Sealing

Signing and Sealing:

- All files in the LandXML zip file MUST be XML files.
- If one must sign and seal a portion of a file, this could be done by placing a ID=”universal unique identifier (UUID)” on the element that defines the portion of the file to sign and seal
- The UUID would prevent possible conflict when files are merged, or XIncluded

LandXML Signing and Sealing

File cross reference Issues:

- LandXML supports element reference provided the reference is in the same file
- Different professionals and sections are going to need to maintain their own LandXML files
- Physically merging files will destroy the files' hash-codes.
- XInclude can be used to reference other XML files

LandXML Signing and Sealing

File Cross Reference Issues:

- XInclude is defined by the W3C, XML Inclusions (XInclude) Version 1.0 (Second Edition)
- The XIncludes would be added to a LandXML file before it was signed and sealed
- The hash-code of the file would reflect that the XInclude elements are present, but would not be affected by any changes to the include file

LandXML Signing and Sealing

Signed/Sealed LandXML files would contain:

- The Professionals personal information
  - License Type
  - License Number
  - Name on License
  - Licensed in State
- Description for signing and sealing
- ID=”Licnse Type”.”License Number”. ”State”.UUID if only a portion is being signed
- XIncludes to merge in needed references

LandXML Signing and Sealing

Signing and Sealing LandXML files:

- An automated process would build the Signature file
- Insure compatibility of information between file
- Test for existence of XInclude files
- Should build only the signature file
- If rebuilding the signature file, report any changes
- Apply Digital Signature

LandXML Signing and Sealing

Signature File Structure:

- Header
  - Processed: Date, Time
  - Professional: Type, Number, Name
  - Description
  - Board Regulation for that State
- Project.Files
  - File
    - Description
    - SHA-1
    - URL
    - ID=”License Type”.”License Number”. License State”. UUID if selecting only a portion of the file
    - XIncludes
      - SHA-1
      - URL
- Digital Signature

LandXML Signing and Sealing

A Sign/Sealed Signature file is VALID when:

- The Digital Signature on the Signature file is valid
- When all the files referenced by the Signature file's:
  - URLs match
  - SHA-1 matches the computed SHA-1
  - Any IDs match what is in the file
  - XIncludes
    - URL
    - SHA-1 matches the computed SHA-1

LandXML Signing and Sealing

LandXML Authentication:

With Signature files and a manifest file one can determine if a file:

- Has been modified
- Is missing
- Has been added after the manifest file was created

If the signature file addresses the issues on Xinclude then the relationship of the Xinclude files to the signed and sealed file could also be verified

LandXML Signing and Sealing

Conclusion:

Applications could be developed that would:

- Automate the signing and sealing process
- Creation of project Identification file
- Creation of the manifest file
- Project validation and authentication
- Assorted project reports
- Zipping and exporting projects

LandXML Archiving

Archiving here refers to long-term storage of the signed and sealed LandXML files.

Long-term in civil engineering terms can look like eternity in the computer world.

Guessing what is happening in the next 5 years for computers is almost impossible, much less 20 years.

LandXML Archiving

What impact does this have on securing signed and sealed files:

- Digital Signatures
  - Get out of date
  - Professional retires
  - Public key cannot be verified
- Attacks on PKI may obsolete the Digital Signature
- Longer hash-codes may be need to maintain security

LandXML Archiving

If the long-term archiving secures the files by their hash-code, independent of the Digital Signature, then there is a way to protect the files long-term.

When the agency that archives the files, for example The Department of Transportation, validates the files by their Digital Signature and then stores the validated hash-code, these hash-codes can be protected by a hash-code tree.

LandXML Archiving

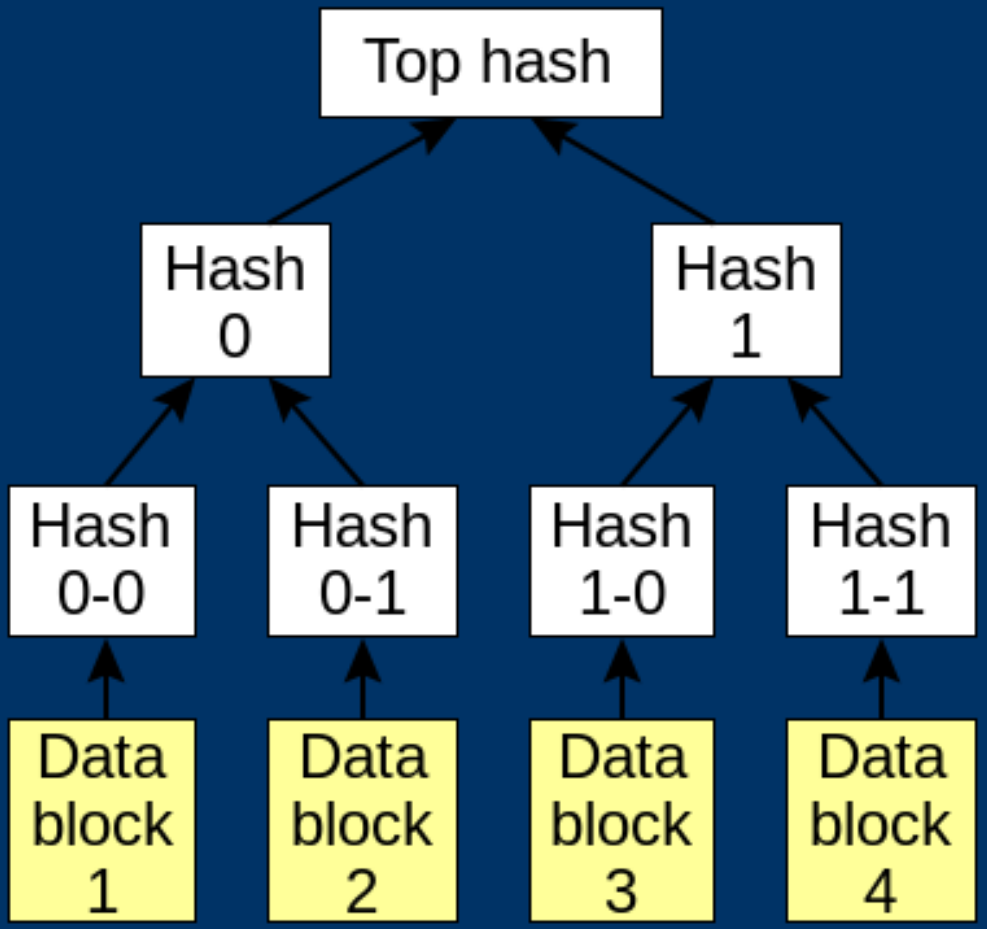
Securing the root of the hash-code tree then protects all the files listed in the hash-code tree. This code could be published in a document in thousands of locations, including libraries.

These archives could be done on a monthly basis, and then combined on a yearly basis.

When computer technology weakens the current hash-code (SHA-1) it could be replaced with a stronger hash-code (SHA256 for example).

LandXML Archiving

Hash Tree:



LandXML Archiving

Long Term Archiving - Architecture:

- All LandXML files renamed by their SHA-1 code
- Stored using the SHA-1 name
- Store project definition file
  - Identification file
  - Manifest file
  - Signature files
- Database:
  - Store projects
  - Extract projects
  - Locate Projects
  - Maintain Project Integrity

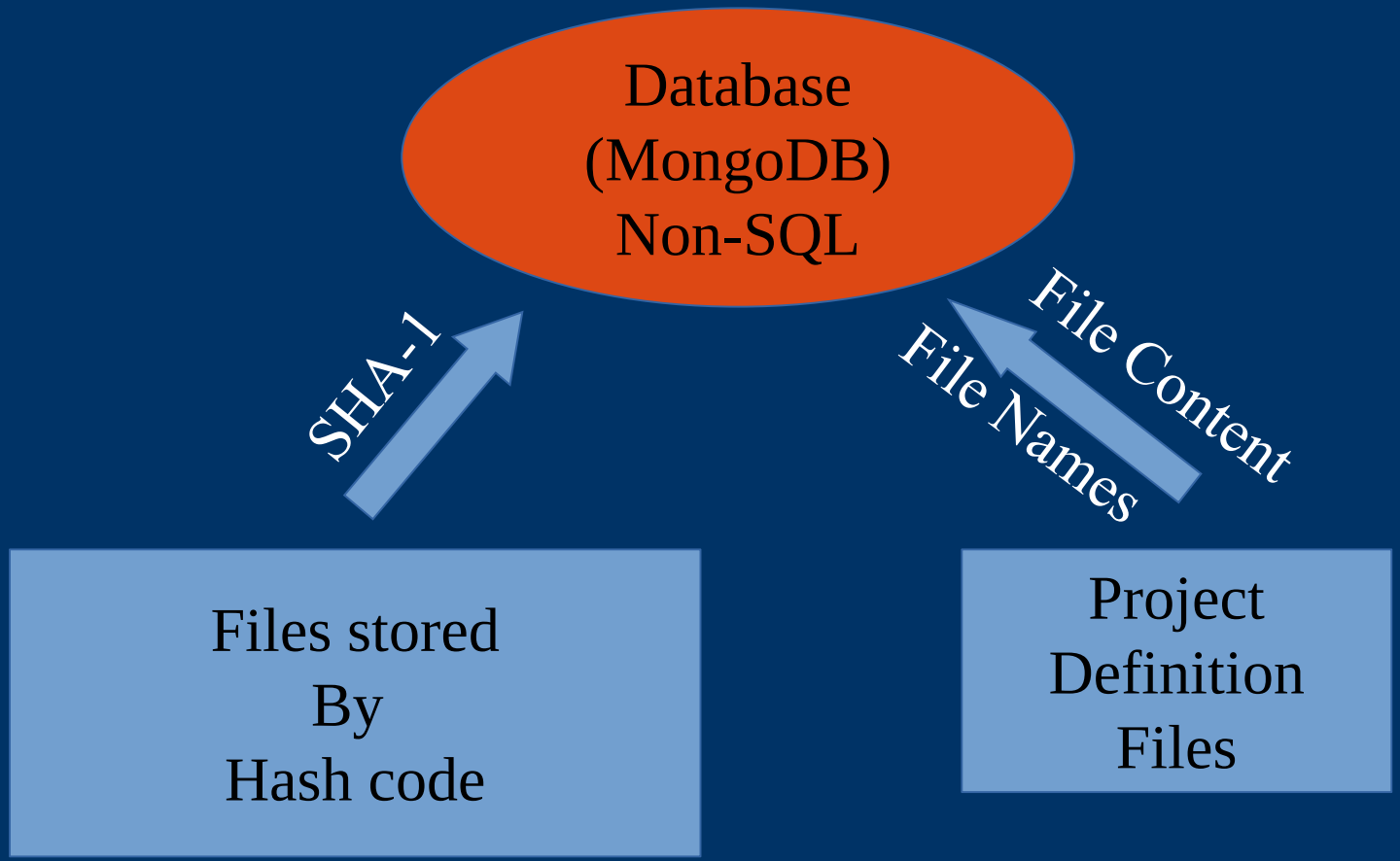
LandXML Archiving

Long Term Archiving – Storage Procedure:

- Validate the structures of the project definition file
- Use digital signature to authenticate manifest file
- Use digital signatures to authenticate all signed and sealed files
- Store all the LandXML files using their SHA-1 as the file name
- If the SHA-1 file name already exists, then the file does not need to be stored
- Store project definition files
- Load database with project definition data

LandXML Archiving

Archiving System Structure:



LandXML Archiving

Long Term Archiving – Extract Project:

- Use database information to locate project
- Create location to store extracted project
- Use Manifest data to locate and extract file
  - SHA-1 to locate the file
  - URL to place and name file
- Locate and extract
  - Identification file
  - Manifest file
  - All Signature files
- Zip extracted project
- Deliver extracted project

LandXML Archiving

Long Term Archiving – Project Integrity:

- Work your way through all project files by their SHA-1 file name
- Compute the SHA-1 of the file
  - If it matches the file name, then it is valid
  - If a mismatch
    - Report error
    - List all projects that contain this file
- This process is repeated on a regular basis

LandXML Archiving

Long Term Archiving – Additional Comments:

- A hash-code tree can be used to secure all the SHA-1 hash codes independent of the Digital Signatures
- The hash-code tree is secured by securing its root hash-code, published in journal, etc.
- Before the SHA-1 hash-codes become obsolete, stronger hash-codes (SHA-256) can be computed and stored
- All stored projects could be recreated independent of the archiving database