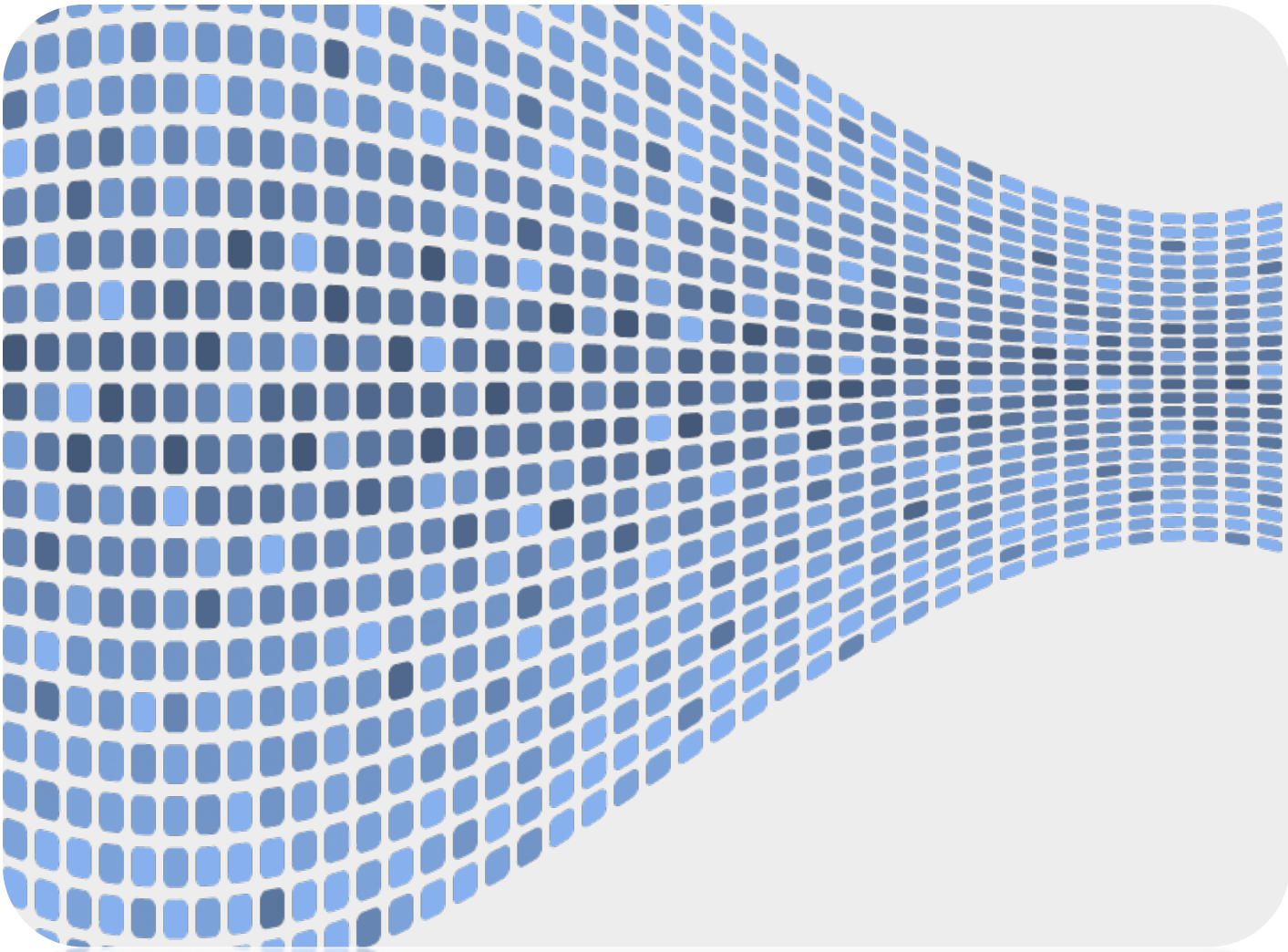


OREGON STATEWIDE LONGITUDINAL DATA SYSTEM P-20W PROJECT

January 31, 2017

Version 1.5

OR-SLDS P-20W SECURITY OVERVIEW

TABLE OF CONTENTS

Revision History

Date	Version	Description	Author
8/25/2016	1.0	Document Initiation	D. Domagala
10/3/2016	1.1	Content Enhancements, still in draft form	D. Domagala
10/10/2016	1.2	Security Requirements section updates to include “solution” column	D. Domagala
10/20/2016	1.3	Revisions made to all document	M. Rebar
11/21/2016	1.4	Revisions made to document	T. Brown
1/30/2016	1.5	Revisions made to document	M. Rebar

Approval

Role	Name/Title	Signature	Date
Project Champion			
Project Director			
System Architect			
Project Manager			

OR-SLDS P-20W SECURITY OVERVIEW DOCUMENT

1. DEFINITION

The Security Overview Document outlines functions and features to protect the Personally Identifiable Information (PII) contained within the OR-SLDS system. This document is intended to provide a non-technical overview of security features and safeguards. Security methods and procedures are described, along with the planned approach to fully meet and exceed security requirements for the OR-SLDS system.

2. SECURITY OVERVIEW

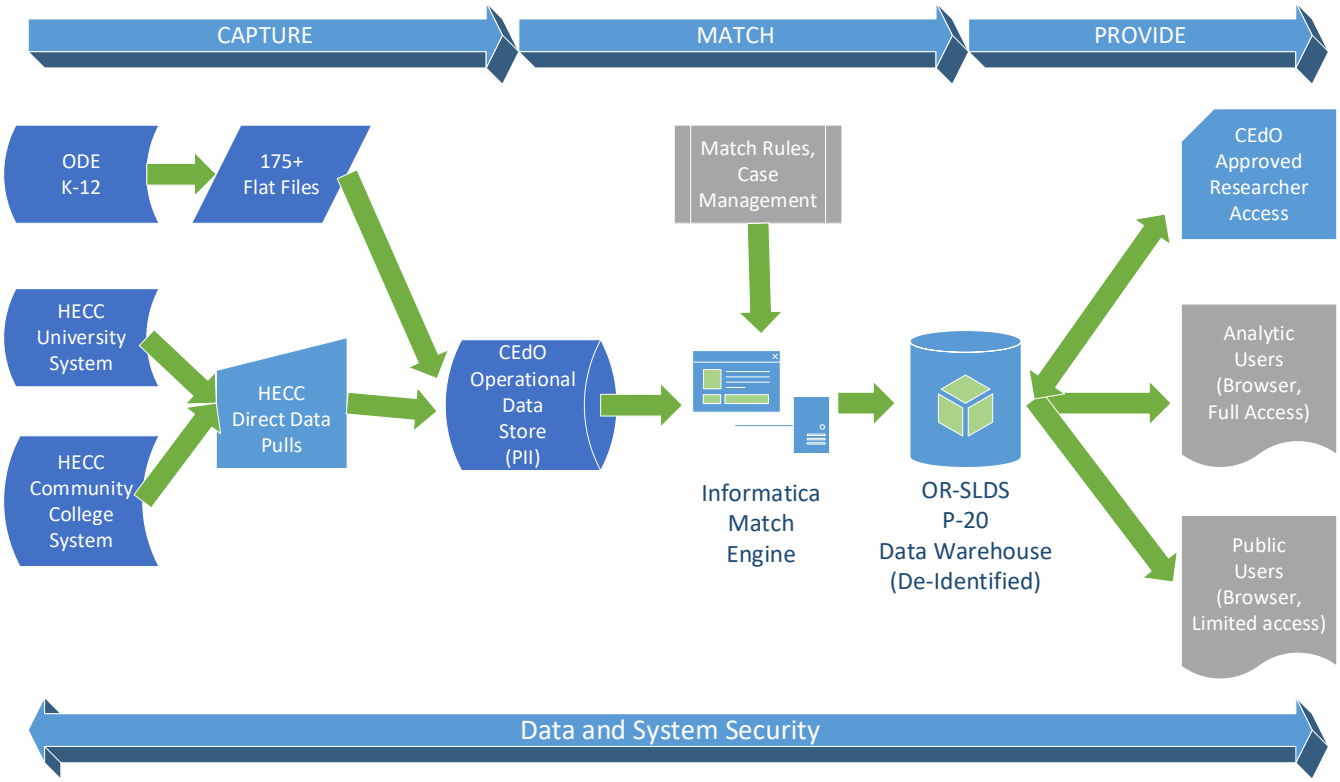
The Oregon Statewide Longitudinal Data System project team (OR-SLDS) will ensure federal statues such as HIPAA and FERPA, and federal standards (such as those published by NIST and FIPS) protections are enforced and personally identifiable information is protected at rest and in transit. Access will only be granted to authorized and authenticated personnel.

Where applicable, as directed by the Chief Education Office (CEdO) and in accordance with FERPA, HIPAA and other legal requirements, database encryption will be applied to protect confidentiality of data at rest. Database access and administration privileges will be restricted to only those explicitly approved by the Chief Education office using role-base authorization and password authentication.

Firewalls, anti-virus software, monitoring tools, and other existing security protections will be fully unitized, or installed as needed to meet the security guidelines established by the Chief Education Office. The OR-SLDS system will abide by all applicable security standards as outlined in Oregon's Enterprise Information Technology Policies.

All data handled by contracted personnel will be handled securely and confidentially, in accordance with federal, state, CEdO, ODE, HECC, and Oregon Enterprise Information Technology Policies.

3. DATA SECURITY



The above diagram depicts the initial data flow for the OR-SLDS system. Over time, a direct connection is anticipated between all source systems and the OR-SLDS Operational Data Store (ODS). Until that time, flat files will be generated by ODE and HECC, and securely provided to the OR-SLDS team for loading into the ODS. The OR-SLDS system shall integrate with data fed from Agency and Partner Agencies' source systems in pre-defined XML and flat file formats, provide identity resolution and management, provide granular storage of longitudinal data (e.g., Operational Data Store), and provide a data warehouse for periodic data snapshots to be exposed in a rich presentation/visualization layer.

CAPTURE

The primary data flow objective within the 'Capture' phase is to securely move data from source systems to an Operational Data Store (ODS). For PK-12 data, the sole source is the Oregon Department of Education (ODE). Eventually, a direct-access route will be commissioned to securely and systematically pull data from ODE systems into the CEdO Operational Data Store. In the interim, numerous flat files will be generated by ODE and securely delivered to an authorized staging area within the CEdO OR-SLDS environment. These 'raw' flat files are then validated and loaded (via Informatica ETL routines) to pre-defined database tables within the Operational Data Store.

For Higher Education data, the Higher Education Coordinating Commission (HECC) will provide secure direct access to data in the Student Centralized Administrative Reporting File (SCARF) format. An automated set of routines will pull data into the ODS on a scheduled basis, with the ability to run ad hoc pulls as needed. Data pulls take place over an internal, secure network supported by Oregon Enterprise Technology Services (ETS).

Only authorized system administrators, as determined by CEdO, have access to the data files, the loading routines, and the ODS data structures. Enterprise Technology Services (ETS) administers the secure network used to transmit the data and files. Personally Identifiable Information from ODE and HECC students is securely housed within the Operational Data Store, in order to longitudinally match those students across state systems.

MATCH

The Operational Data Store (ODS) securely houses personally identifiable student data from ODE and HECC. This data is processed through a match engine (powered by Informatica software) using pre-defined match rules. Most matches are systemically confirmed, but some will require manual review by a Case Manager. A Case Manager is authorized by CEdO to review student demographic information and make a determination whether there is a longitudinal match.

Once a match is determined, all state data for that matched student is de-identified and assigned to a “surrogate key” as it is loaded into a secure PK-20 longitudinal database. This de-identified student-level data then forms the basis for researcher analysis and aggregated reporting for Oregon educational outcomes.

PROVIDE

De-identified records for Oregon students are stored in a secure Data Warehouse, on physical servers within the State Data Center. Only authorized personnel from the Oregon Enterprise Technology Services team have physical access to the Data Warehouse servers. Only authorized administrators from the CEdO have system access to the Data Warehouse. And only CEdO authorized researchers and analysts have access to the longitudinal information contained within the Data Warehouse.

A visual analytic tool, IBM Cognos, is utilized by these authorized researchers and analysts to study the information and produce insights into educational achievement and outcomes.

CEdO carefully reviews and explicitly approves any longitudinal reports that are made publicly available. Public reports are aggregated or suppressed at a cell-level to avoid

potential identification of individual students. Suppression guidelines and other security best practices published by the U.S. Department of Education's Privacy Technical Assistance Center (PTAC) are consistently applied and administered by the OR-SLDS project.

4. SOFTWARE SECURITY

This section describes the enabled and configured security features of the two primary software tools for the OR-SLDS system, Informatica and Cognos.

INFORMATICA ROLE SECURITY (Req# 2.6, 2.7, 2.10)

The Informatica Domain utilizes the concept of Security Domains to access content and services. A domain can either be defined with an LDAP (Lightweight Directory Access Protocol) directory or by using the native Informatica domain. These domains are collections of users and groups of users who have been given access the various services either directly or through the use of predefined roles. These configurable roles include, for example,

- Administrator
- PowerCenter Developer
- Business Glossary Consumer

Account management within the Informatica domain allows for configuration of Maximum Login Attempts and locking out individual users (including users with the Administrator role).

MDM ROLE SECURITY (Req# 2.6, 2.7, 2.10)

Role security Master Data Management (MDM) is established by configuring users within the MDM Hub Master Database or by synchronizing groups with an LDAP service. These users or groups are then granted permissions directly or by role to various objects and services within an Operational Reference Store (ORS) using the Security Access Manager (SAM).

Permissions within the SAM can be set on any object within the ORS as Read, Write, Update, Delete, Merge, and Execute.

Integration of the ActiveVOS to Informatica Data Director (IDD) requires the creation of three MDM roles: DataSteward, Manager, and SrManager. These roles are used to manage IDD application task approvals through the ActiveVOS Business Process Manager (BPM). Access to the IDD application is provided as a separate object within the SAM.

Account management within MDM is accomplished using a Global Password Policy where a maximum number of failed logins is configured.

COGNOS ROLE SECURITY (Req# 2.6, 2.7, 2.10)

Cognos leverages Active Directory for authentication. Cognos Role based security is described as user-level security which focuses on the logical role of a user rather than the user's individual identity. The IBM Cognos security model allows you to manage users as member of roles and groups. These groups and roles can be used in Security policies such as access permission for each object within the IBM Cognos portal.

LDAP AUTHENTICATION (Req# 2.5)

LDAP (Active Directory) configuration will be administered by the CEdO. Groups configured within the LDAP service will correspond to the required roles defined within the Cognos, Informatica, and MDM. Synchronizing of Informatica groups with those defined in the LDAP service occurs at a defined time every 24 hours. Manual (on demand) synchronization will be implemented.

5. DATA IN TRANSIT

INFORMATICA (Req# 2.8, 2.9, 2.12)

All data in transit within the Informatica domain is encrypted using the SSL/TLS protocol using 512-bit RSA encryption. Data in transit includes the following data communication pathways between:

- Service Manager and all services running in the domain
- Data Integration Services and associated Model Repository Services
- Data Integration Services and workflow processes (Data Quality)
- PowerCenter Integration Services and PowerCenter Repository Services
- Domain services and the Informatica client tools and command line programs

Data in transit from CEdO users accessing Informatica web application services is encrypted using the SSL/TLS protocol using 512 bit RSA encryption and accessible on specific ports. These services include:

- Analyst Service
- Web Services Hub Console Service
- Metadata Manager Service

Data in transit from remote agencies including ODE and HECC will utilize secure database connections over the SSL/TLS protocol using 512 bit RSA encryption. Data in transit from local (CEdO) databases including the various Informatica domain repositories, ODS, and data warehouse does not use secure database connections, but

travels only within a secure internal network maintained and monitored by the Oregon state data center.

MDM (Req# 2.8, 2.9, 2.12)

Data in transit within the MDM services is encrypted using the SSL/TLS protocol using 512 bit RSA encryption. Data in transit includes communication between the MDM Hub Service, Process Server, and ActiveVOS BPM (Business Process Manager) server.

Data in transit from local (CEdO) databases including the Hub master database, the ORS databases, and the ActiveVOS database as well as the ODS and data warehouse databases does not use secure database connections.

Data in transit from web accessible IDD application services is encrypted using the SSL/TLS protocol using 512 bit RSA encryption and accessible on specific port.

COGNOS (Req# 2.8, 2.9, 2.12)

Data in transit from client to web server is secured via SSL certificate in IIS. Data in transit between Cognos processes is encrypted using SSL.

6. DATA AT REST

TDE – TRANSPARENT DATA ENCRYPTION (Req# 2.1)

All databases running within the local (CEdO) network will have Transparent Data Encryption (TDE) enabled or other robust encryption for data at rest.. These databases include the various Informatica domain repositories, MDM ORS and service repositories, Cognos content store, ODS and data warehouse. CEdO configures and administers TDE on the local SQL Server databases.

UNIT RECORD AUDITING (Req# 2.4)

Unit record auditing is configured on all databases holding or potentially housing personally identifiable information (PII). CEdO configures and administers unit record auditing on the local SQL Server databases to determine when a record was last updated, and by whom.

7. SECURITY REQUIREMENTS

The comprehensive list of contractual business requirements can be found in Contract #DASPS-1416-16, Exhibit J. Security-specific requirements have been culled from the full list and provided here for reference.

Data and System SECURITY Requirements

Req #	Description	Solution
2.1	Robust encryption of data at rest (database, tables, files).	Utilize Transparent Data Encryption (TDE) at the SQL Server database level to encrypt data
2.2	Robust encryption of data in transit.	Data in-transit processes can be controlled by the security provided at the connection object level. The Informatica Platform supports administrative authorities with a hierarchical security model with privileges and permissions configurable at the user, folder, group, and repository levels. It also provides integration with LDAP for authentication and FIPS 140-2 certified encryption for securing data in flight through industry standard algorithms like AES, Base 64, CRC32, MD5, and RC5 for SSL-based encryption. This ensures that no unauthorized person can use a connection object created by someone else to pull out restricted information in transit or otherwise from a data source. Use of OS Profiles allows different jobs to run under different OS user accounts. In this way, the PowerCenter engine can only access data as allowed by the OS profile user account. The product is also DOD compliant and runs on NIPRNET, SPRNET, and JWICS. There are more than 130 projects installed at DoD entities like Tricare, VA Hospitals, Air Force Surgeon, Army Medical Services, CMS, FDA, DLA, Army, Navy, and Air Force. IBM Cognos can be configured to encrypt data in transit at any point. Between the end user and the web server, it is securable and encrypted using standard SSL/HTTPS standards and certificates. In addition, data being transferred from application services to web services can be encrypted using an IBM-provided, SSL-based KeyStore.
2.3	Support for two factor authentication.	IBM Cognos provides the ability to create custom authentication providers (CJAPs) in Java. Using a CJAP, you can create a Trusted Signon Provider, which can be further extended to support a wide variety of

Req #	Description	Solution
		authentication/ authorization sources, including integrating with a two-factor authentication system. The Informatica domain can use the following types of authentication to authenticate users in the Informatica domain: • Native user authentication • LDAP user authentication • Kerberos network authentication Native user accounts are stored in the Informatica domain and can only be used within the Informatica domain. Kerberos and LDAP user accounts are stored in an LDAP directory service and are shared by applications within the enterprise.
2.4	Support granular auditing of access to unit records with personally identifiable information (ODS and identified Warehouse).	The IBM Cognos solution comes with a complete audit database, which can be configured to provide access information at a session, object, and user level.
2.5	Supports LDAP authentication via TLS and SSL and LDAP integration for password security (timeouts, account disabled, etc.). Provides simplified sign on capability to users. Describe in comments.	Both Informatica and IBM Cognos can be configured to integrate with LDAP and can be implemented with single sign-on so end users who are already authenticated pass seamlessly into their desired reports.
2.6	Provides pre-set role and custom role-based authentication.	Both products can utilize LDAP groups or configure their own internal groups and roles to facilitate access restriction protocols.
2.7	Control access to application functions through user roles.	Both products can utilize LDAP groups or configure their own internal groups and roles to facilitate access restriction protocols.
2.8	Web applications use TLS/SSL/HTTPS for data encryption and secure handshake.	IBM Cognos provides support for those protocols at all levels of the architecture. Standard SSL/HTTPS techniques are used to secure the browser and application server

Req #	Description	Solution
		communication. More can be read regarding the TLS support at http://www-01.ibm.com/support/knowledgecenter/SSEP7J_10.2.0/com.ibm.swg.ba.cognos.vvm_user_guide.10.2.0.doc/c_vv_transportlayersecuritytls_96539.html%23VV_TransportLayerSecurityTLS_96539. You can enable options in the Informatica domain to configure secure communication between the components in the domain and between the domain and client components. Informatica uses the TCP/IP and HTTP protocols to communicate between components in the domain. The domain uses SSL certificates to secure communication between components. You can enable different options to secure specific components in the domain. You do not have to secure all components in the domain. For example, you can secure the communication between the services in the domain but not secure the connection between the Model Repository Service and the repository database. When you install the Informatica services, you can enable secure communication for the services in the domain and for the Administrator tool. After installation, you can configure secure communication in the domain from the Administrator tool or from the command line. You can set up secure repository databases and secure source and target databases. You can also secure the connection between Informatica web application services and browsers.
2.9	Any additional web components (e.g., web service) are secured through SSL.	Within Cognos, SSL can be configured to support any internal connections, external connections, or both

Req #	Description	Solution
		You can enable options in the Informatica domain to configure secure communication between the components in the domain and between the domain and client components. Informatica uses the TCP/IP and HTTP protocols to communicate between components in the domain. The domain uses SSL certificates to secure communication between components. You can enable different options to secure specific components in the domain. You do not have to secure all components in the domain. For example, you can secure the communication between the services in the domain but not secure the connection between the Model Repository Service and the repository database. When you install the Informatica services, you can enable secure communication for the services in the domain and for the Administrator tool. After installation, you can configure secure communication in the domain from the Administrator tool or from the command line. You can set up secure repository databases and secure source and target databases. You can also secure the connection between Informatica web application services and browsers.
2.10	Delivers security rules such as maximum number of incorrect login attempts, session timeout. Describe in comments.	Cognos security rules are implemented at different parts of the application depending on the specific requirement. Between the authentication provider (LDAP, Active Directory, etc.) and IBM Cognos's configuration, there are very few limitations. In the example provided, "maximum number of incorrect login attempts" would be managed at the authentication provider level, which is inherited and honored by IBM Cognos. The "session timeout" would be configured in Cognos Configuration where the web

Req #	Description	Solution
		session's token is invalidated once the defined timeout is reached. To improve security in the Informatica domain, an administrator can enforce lockout of domain user accounts, including other administrator users, after multiple failed logins. The administrator can specify the number of failed login attempts a user can make before the user account is locked. If an account is locked out, the administrator can unlock the account in the Informatica domain. When the administrator unlocks a user account, the administrator can select the "Unlock user and reset password" option to reset the user password. The administrator can send an email to the user to request that the user change the password before logging back into the domain. To enable the domain to send emails to users when their passwords are reset, configure the email server settings for the domain. If the user is locked out of the Informatica domain and the LDAP server, the Informatica administrator can unlock the user account in the Informatica domain. The user cannot log in to the Informatica domain until the LDAP administrator also unlocks the user account in the LDAP server.
2.11	Can provide a documented policy for "hardening" the operating system for web and other servers.	There are several articles and whitepapers describing securing the application as well as the operating system and services. One example is this: http://www.ibm.com/developerworks/data/library/cognos/security/cognos_bi_platform/page602.html. In general, IBM Cognos does not use port ranges and supports the best practices used for the specific operating system (Windows, Linux, Unix, etc.) and web server (IIS, Apache, etc.).

Req #	Description	Solution
2.12	Web applications use TLS/SSL/HTTPS for data encryption and secure handshake. (duplicate of 2.8)	Please see 2.8 You can enable options in the Informatica domain to configure secure communication between the components in the domain and between the domain and client components. Informatica uses the TCP/IP and HTTP protocols to communicate between components in the domain. The domain uses SSL certificates to secure communication between components. You can enable different options to secure specific components in the domain. You do not have to secure all components in the domain. For example, you can secure the communication between the services in the domain but not secure the connection between the Model Repository Service and the repository database. When you install the Informatica services, you can enable secure communication for the services in the domain and for the Administrator tool. After installation, you can configure secure communication in the domain from the Administrator tool or from the command line. You can set up secure repository databases and secure source and target databases. You can also secure the connection between Informatica web application services and browsers.