Smarter Balanced Reporting (RFP 15)
Security Overview

Prepared for:

by:

Approvals

Representing	Date	Author	Status
Consortium		Joe Willhoft	
Consortium	2014.09.24	Brandt Redd	Approved for Milestone 5
PMP	2014.09.24	Kevin King	Endorsed for Milestone 5
Workgroup	2014.09.23	Henry King	Endorsed for Milestone 5

Revision History

Revision Description	Author/Modifier	Date
Initial Release (DRAFT)	Anna Grebneva (Amplify)	2014.07.09

Table of Contents

Smarter Balanced Data Warehouse and Reporting Security Overview

1 Summary

There are multiple security layers to protect PII housed by Smarter Balanced Reporting and Data Warehouse systems.

PII is protected in three states:

- Data in use - data exposed to end users.
- Data in transit - data in transit over networks.
- Data at rest - data stored in file systems ,etc.

1.1 Data in Use

Data in use is protected by applying proper roles and permissions as well as identifying and controlling of what data is accessible within user scope. The last control is referred in this document as *context security*.

1.2 Data in Transit

Data traveling across networks is protected by using secure channels, such as Secure Sockets Layer (SSL) and HTTPS.

1.3 Data at Rest

PII is stored on a file system in an encrypted state. This is achieved by either encrypting individual files or using an encrypted file system. Smarter Balanced Reporting and Data Warehouse uses both approaches.

2 Reporting System

2.1 Roles and Permissions

Roles and Permissions are provided to Smarter Balanced Reporting by the response from the Smarter Balanced Single Sign-On (SSO) service. During user authentication, the service returns all the necessary information for the Reporting System to make decisions about user access rules and context.

Smarter Balanced Reporting has seven defined permissions that correspond to different feature authorization access, as opposed to a multitude of differentiated roles. The permissions are defined in the table below.

Permission	Description
GENERAL	All users authenticated from SSO service are given the General permission. General permission grants users access to non-PII reports, namely, Comparing Populations Report at state, district and school level.
PII	Users with PII permission are authorized to reports containing PII data. These reports include List of Students, and Individual Student Report, as well as Batch Print feature.
ALLSTATES	Users with All States permission are considered “Consortium level” users. With this permission, the user has access to all the tenants/states of an install. This access is restricted to non-PII reports.
SAREXTRACTS	Users with SAR Extracts (Student Assessment Result Extracts) permission are authorized to perform CSV extraction for student assessment data.
SRSEXTRACTS	Users with SRS Extracts (Student Registration Statistics Extracts) permission are authorized to perform CSV extraction for student registration statistic data.
SRCEXTRACTS	Users with SRC Extracts (Student Registration Completion Extracts) permission are authorized to perform CSV extraction for student registration completion data.
IIRDEXTRACTS	Users with IIRD Extracts (Individual Item Response Data Extracts) permission are authorized to request the statewide item response data for a given assessment; this permission is intended to support psychometric analysis
AUDITXML	Users with Audit XML permission are authorized to request the original source files from Test Integration for a given assessment;

	this permission is intended to support auditing of data and storage (or subsequent processing) of data in addition to those already persisted in the other Data Stores.

Entity Relationship (a.k.a. Tenancy Chain) describes the relationship between a user and the permission within an institution hierarchy. A user may be granted permission to a particular school, district, state, tenant or consortium. It is expected that at least one entity relationship exist for every user. Each authenticated user is automatically granted General permission, with which they can view aggregate non-PII reports. Roles/Permissions that are not recognized by the Reporting System are ignored and are replaced with General permission.

Smarter Balanced Reporting expects the format of the entity relationship to be in:

|RoleId|**RoleName**|Level|ClientID|Client|GroupOfStateID|GroupOfStates|**StateID**|**State**|GroupOfDistrictsID|GroupOfDistricts|**DistrictID**|District|GroupOfInstitutionsID|GroupOfInstitutions|**InstitutionID**|Institution|

Note: The highlighted fields are the attributes that Smarter Balanced Reporting use for authorization.

Name	Index	Description	Example Value
RoleName	1	Role/Permission	PII
StateID	7	Tenant Name	North Carolina
State	8	State Code	NC
DistrictID	11	District ID	4218c017-8093-458f-8045-ac9d3306466c
InstitutionID	15	School ID	13e9c2ae-4621-4d2b-b770-2a569e078c96

2.1.1 Consortium Level Access

a user with consortium level access for a particular permission has an entity relationship with empty values for StateID, State, DistrictID and InstitutionID. This use will have that permission for all data in that deployment (i.e., all States, Districts, and Schools).

2.1.2 State Level Access

a user with state level access for a particular permission has an entity relationship with StateID and State values. This user will have that permission for all Districts and all Schools within that State.

2.1.3 District Level Access

a user with district level access for a particular permission has an entity relationship with StateID, State and DistrictID values. This user will have that permission for all schools in the specified District.

2.1.4 School Level Access

a user with school level access for a particular permission has an entity relationship with StateID, State, DistrictID and InstitutionID values. This is the finest grain of permission control.

2.2 Context Security

PII data is restricted and protected based on the user's permission derived from his entity relationships. We protect data in several ways.

Prior to every database access, the application validates that the source database to which the request needs access is associated to the user's tenants/states. The application forbids users from accessing databases that are outside of the user's tenants/states.

Context is also applied to database queries, protecting PII data that a user doesn't have permission to. Technically, based on the user's entity relationships, SQL "WHERE" clauses are appended to queries that solate the result sets returned by the database. For instance, if a user only has PII access to School ABC, the SQL "WHERE" clause that gets appended to the query will restrict the results for school ABC. If this user tries to access School XYZ, the results from the query will be an empty set as the Select statement will contain a "WHERE" clause for "School equals to ABC" and a second where clause for "School equals to XYZ". Such request always produces an empty set of result as the "WHERE" clauses produce disjoint sets.

The following query illustrates the example above with the context condition underlined:

```
SELECT column
FROM table
WHERE school='XYZ'
AND state='NC'
AND district='123'
AND school='ABC'
```

2.3 Reporting Components Security

2.3.1 Web Application

The web application is one of two points of access to PII. It is responsible for calculating user context rules and enforcing them. Configuration is required to integrate properly with platform and component-internal services.

2.3.2 PDF and Batch Print

The storage of PDFs are on an encrypted file system. PDF requests are restricted to users with PII permission and context security is applied to the database query for data retrieval. Bulk PDF requests for Batch Print can only be downloaded by the requested user. The PDF service is accessible via Web Application.

2.3.3 Extracts

Extract service is internal and only accessible via Web Application. The storage used by the service is on an encrypted file system. Extracts can only be requested by users with the corresponding extract permission and context security is applied to the database query. The resulting extracts will be transferred to the Pickup Zone.

2.3.4 Read Only Data Stores

The storage of data in Read Only Data Stores are on an encrypted file system. Data Stores are tenant/state-based and access is limited to users that are affiliated to the tenant/state.

2.3.5 Pickup Zone

Files in the Pickup Zone are on an encrypted file system. The file can only be picked up by the authenticated original requestor of the file, and are served via HTTPS.

3 Data Warehouse

3.1 Data Warehouse Components Security

3.1.1 Landing Zone

Landing Zone Users have the ability to SFTP data files into Landing Zone using public key authentication. The expected data files must encrypted using GPG by the user before transferring over the secured channel.

3.1.2 Data Loader

Data Loader copies files from Landing Zone to an encrypted file system. Data Loader servers are internal to the system hence have no user access. Data Loader decrypts the data file using the corresponding tenant's public key and verifies the signature of the file. If the signature fails, then the file is rejected.

3.1.3 Data Migrator

Data Migrator does not use any temporary storage to migrate the data. The data origin and target destinations are data stores on an encrypted file system.

3.1.4 Read Write Data Stores

The storage of data in Read Write Data Stores is on an encrypted file system.

4 Security Event Audit

Smarter Balanced reporting system logs each security event, such as PII requests.

The following is an example audit log entry for a user with PII and General permission that accessed List of Students Report,

{"asctime": "2014-07-01 11:06:31,808", "msg": {"principals": ["PII", "GENERAL"], "callable": "get_list_of_students_report", "session_id": "5e5ac3f1-df9d-48cd-8f25-b74f18dc1f9c", "params": {"args": {"params": {"asmtGrade": "8", "stateCode": "NC", "districtId": "228", "schoolId": "245", "asmtYear": 2016}}}}}

5 Security Test

Amplify uses a simple algorithm to determine the risk ranking, the likelihood of a vulnerability multiplied by its impact. Likelihood is defined as the probability that an attacker can exploit the issue. Impact is the perceived damage done to the asset or application if the issue is exploited.

Amplify uses five risk rankings, described below.

	Severity			
Impact	High	Medium	Medium-High	High
	Medium	Medium-Low	Medium	Medium-High
	Low	Low	Medium-Low	Medium
	Low	Medium	High	
	Likelihood			

All medium, medium-high, and high severity issues need to be resolved. High and medium-high issues must be resolved before release. Medium-severity issues may need to be fixed before release, or released as part of a subsequent update, depending upon the nature of the issue.

Risk Ranking Examples

Risk	Likelihood	Impact	Severity
Coding error allows student to easily view inappropriate	High	High	High

content			
Out-of-date server software can be exploited by skilled hacker to gain access to lesson plans	Medium	Low	Medium-Low
Coding error allows teacher to view student data for students not in her class (but in her school)	Medium	Medium	Medium
Weak encryption enables student data to be extracted from lost tablet	Low	High	Medium

Amplify completed information security audits prior to each beta iteration releases. These audits typically included the following types of tests: security code review and web application penetration testing which are focused on the changes made for any given code release. This involved a combination of manual and automated techniques to attempt to circumvent an application's permission model to undermine the confidentiality, integrity, or availability of data. The audits did not include the review of operational controls or hosting environments. Amplify recommends that Smarter Balanced Assessment Consortium continue to follow standard industry practices for secure application development and operations going forward.