Information Paper

Management of Security for Access, Data and Documents within AWARD®

John Crickmore, Managing Consultant

Commerce Decisions Pty Ltd

"Helping people around the world benefit from the right procurement decisions being made on important projects"

Contents

List of Figures

List of Tables

Introduction

Commerce Decisions launched its unique hosted evaluation system AWARD® in 2001, to streamline and improve the processes used by organisations to evaluate tenders. The use of AWARD® has enabled over 200 clients, for acquisitions exceeding a total of $400 billion, to access several benefits including:

- Sped up the whole procurement process from initial tendering through to contract award
- Gave visibility of the whole process and provided a clear and easily accessible audit trail
- Powerful document management and search capabilities enabled rapid access to information contained in multiple and large documents
- Being web-enabled, AWARD® allowed an unlimited number of stakeholders to work and provide their input at their own pace, as and when they wished
- Reports and analysis could be easily generated and were available in real time and on demand
- Enabled rapid and fast updates on the progress of the bid process
- In built audit trails provided full visibility of the evaluation processes, enabling any challenges to be successfully met.

However, the use of AWARD® is vastly different to the traditional method of spreadsheets and paper in a locked room, which can create concerns that using a hosted service such as AWARD® might expose the organisation to unnecessary risks around:

- Access by evaluators to AWARD® from different locations
- Security of the documents held in AWARD®
- Security of the answers being recorded in AWARD®
- Electronic handling of documents from within AWARD®
- Unauthorised access to AWARD® by other parties.

In the 15 years that AWARD® has been available to clients, these concerns have been raised, and Commerce Decisions has demonstrated that through its established processes, controls within AWARD®, oversight of related parties such as Data Centre, and advice on how the client can manage their processes, those concerns can be addressed adequately.

In the Australian context, Commerce Decisions has been supporting the evaluation of complex and high-value acquisitions since 2013. Most of these have been for the Department of Defence, with highly sensitive material, numerous documents and evaluators, and oversight from the Australian Government Solicitor (AGS).

There have been no issues related to security of the information held within AWARD®, which is managed and monitored in a proactive manner including:

- AWARD® is hosted in an Australian Signals Directorate (ASD) certified data centre, with all staff holding current security clearances
- Strict access controls within AWARD® (username & password), that controls who can access the evaluation projects within AWARD®, and the role they are assigned to
- Event logs within AWARD® that can be searched to provide information on the activities of users, including which documents they have accessed
- Proactive monitoring of the AWARD® server logs, providing weekly reports on which IP addresses users have logged in from.

This Information Paper has been prepared to provide an overview of how the security design and practices

Overview

Use of AWARD® in the Australian Government sector

AWARD® is used extensively in the Government sector, with several government agencies using AWARD® on an enterprise level, to support the procurement of its equipment, platforms and services. These include:

- UK Ministry of Defence
- UK Transport for London
- High Speed 2 (HS2) Rail Project
- CrossRail Underground Rail Development
- Highways England

The first project in Australia using AWARD® was conducted in 2013 for the Dept of Defence - Maritime Systems Division. Since then, AWARD® has been used to support four more tender evaluations within Defence, with another three currently in progress. These projects range from large, complex procurement of capability (approx. $2 billion) through to service panels managing several hundred responses across 12 service categories. Commerce Decisions has also completed a pilot evaluation activity with the Melbourne Metro Rail Authority (MMRA), with the aim of using AWARD® on a broader basis within MMRA.

Through the work for Government in Australia, Commerce Decisions has complied with all requirements and processes around probity, information security, document security and record keeping/auditing.

Australian Data Centre Provider

AWARD® is hosted in a secure, accredited data centre that meets Australian Government and Defence information security requirements. This service is currently provided by Sliced Tech, with the data centre being in Canberra, ACT.

Sliced Tech was an inaugural member of the Federal Government's whole-of-government cloud services panel, and currently provides cloud services to several Federal Government departments and agencies in Canberra, including the Department of Finance, Department of Education and Training, Clean Energy Regulator, and National Archives of Australia.

Sliced Tech's facilities and information systems are assessed against the standards published by the Australian Signal Directorate (ASD) – refer to Attachment A and Attachment B. Sliced Tech's personnel are based in Australia, and hold Australian Government Security Clearances.

Commerce Decisions makes use of Sliced Tech as a data centre provider, as its facilities are rated to UNCLASSIFIED-DLM, which is sufficient for most tender evaluations. If required, Sliced Tech can provide environments rated to higher classification, but this has not been necessary for the work Commerce Decisions has conducted in Australia.

Security Architecture

Overview

AWARD® is a web-enabled solution, that is accessible via a web browser from the User's location. As shown in Figure 1 below, there are several elements in the architecture that relate to security, and the protection of the data within AWARD®.
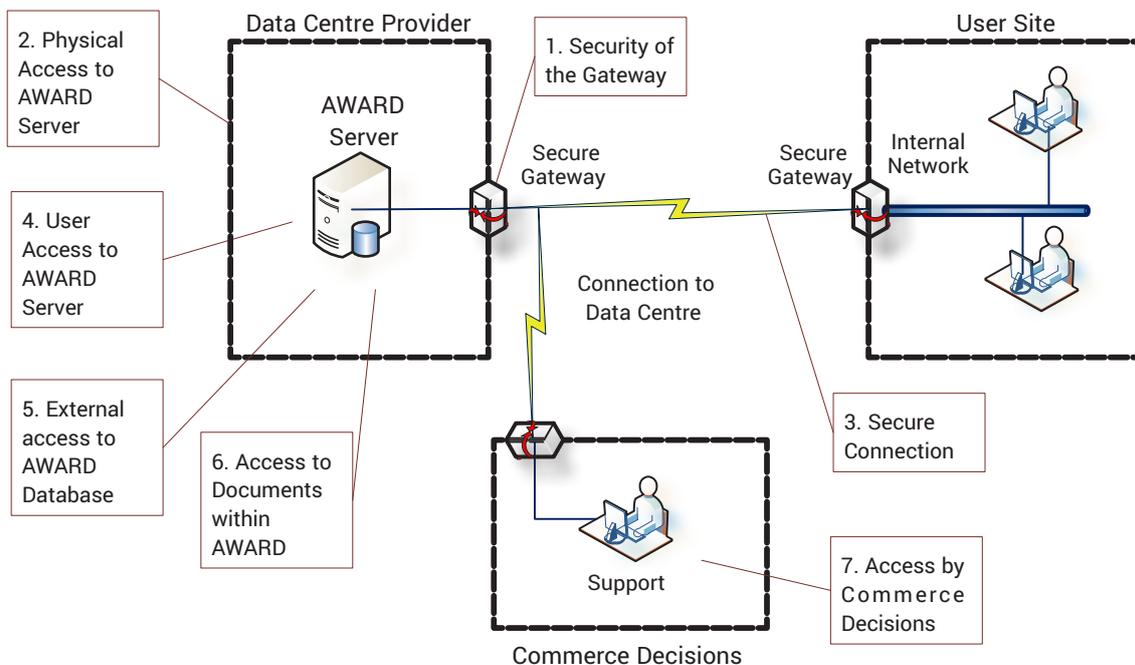

Figure 1: Security Overview

As illustrated in Figure 1 above, there are seven specific elements that are addressed to ensure the security of the data and documents within AWARD®; which can be grouped under two main categories:

- External Security
    1. Security of the Internet Gateway to access AWARD® in the Data Centre
    2. Physical Access to the AWARD® Server
    3. Secure connectivity between the Data Centre, and the User Site and Commerce Decisions in Australia
- Internal Security
    4. User Access to the AWARD® System
    5. External access to the AWARD® Database
    6. Access to Documents within AWARD®
    7. Access by Commerce Decision Support

The management of these elements rests with Commerce Decisions, although the security for the first two elements above is delivered through the contractual relationship with the Data Centre provider.

The processes and approach to that management is detailed in the following sections.

AWARD® Configuration

The AWARD® server can support any number of Clients. For each Client, a specific Account is created by Commerce Decisions within AWARD®. A new instance of the database is created for each Account, ensuring complete separation of the data. As shown in Figure 2 below, once the Account is created, any number of evaluation Projects can be created.
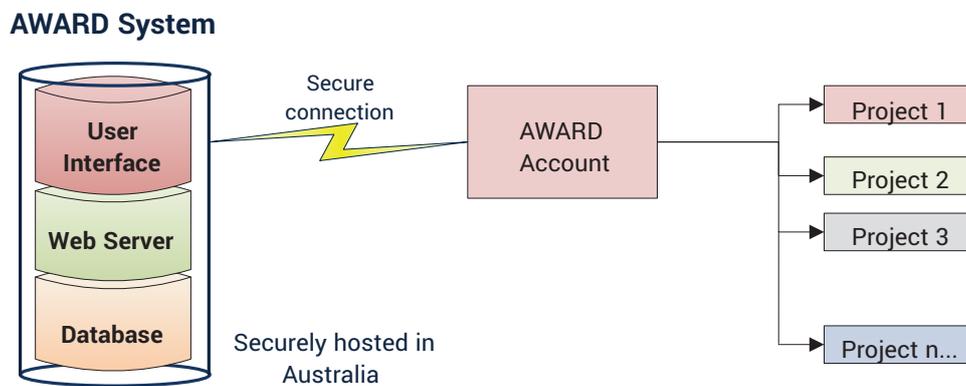

Figure 2: AWARD Configuration

The administration of AWARD® is conducted at the Account and Project levels as detailed in Table 1

Table 1: User Roles

Level	Role	Ability	Notes
Account	AWARD® Administrator	Grants full Account Administrative rights	Only allocated to Commerce Decisions Aust personnel
	Create Project	Allows User to create new Projects and configure them	Sometimes this is provided to the Client's Administrator, so they can create new Projects
Project	Assessor	Allows the user to submit answers	For Evaluators and Moderators who only answer questions
	Project Support	Grants the user partial control over a project's setup	Provided to Evaluation Managers, so they can run reports, add users and assign questions
	Project Manager	Grants the user full control over a project's setup	Provided to Client's Administrators to enable them to change the project configuration if required
	Stakeholder	Provides the user read access to the full project	Usually provided to SME's or probity advisors

The Account roles are only assigned to Commerce Decisions personnel who are authorised to access the data, which includes Tenderers' responses. Access is restricted to solely Australian based personnel who have completed the necessary Conflict of Interest forms and hold the appropriate security clearance e.g. at least BASELINE.

The Project roles are assigned as identified in the project requirements. Generally, the Project Manager role is not assigned to the Client, to avoid any un-intended changes to AWARD® during the conduct of the evaluation.

Security Management

Security of the Internet Gateway to access AWARD® in the Data Centre

AWARD® is hosted within the data centre provided by Sliced Tech. Sliced Tech have their internet gateway accredited against ASD's standards, for use up to PROTECTED as per the Australian Government security classification scheme.

Given the material being transmitted to and from, and held within AWARD® is UNCLASSIFIED-DLM e.g. SENSITIVE: COMMERCIAL, the level of accreditation of the Gateway is sufficient for the purposes of conducting tender evaluations

A copy of that certification is included as Attachment A.

Physical Access to the AWARD® Server

Sliced Tech provides an Infrastructure-As-A-Service (IaaS) platform for the hosting of AWARD® within their data centre. Sliced Tech's Cloud Services have been accredited against ASD's standards for hosting of information up to UNCLASSIFIED-DLM. As noted above, the information being transmitted to and from, and held within AWARD® would be classified no higher than UNCLASSIFIED-DLM e.g. SENSITIVE: COMMERCIAL.

A copy of that certification is included at Attachment B.

Sliced Tech delivers cloud based services for several Federal and State Government departments – IaaS/ PaaS, who have similar confidentiality requirements to those of Defence e.g. Dept of Finance. As such, Sliced Tech's personnel are based in Australia, and hold Australian Government Security Clearances. Sliced Tech maintains processes and procedures to ensure the security of the information held within its data centres, and prevent unauthorised access to any client information.

Secure Connectivity with AWARD®

The connection to AWARD is managed through a secure encrypted link (2048 bit), as used in the Security and Banking sectors. This is provided through Symantec, as a trusted supplier of encryption services. The "Certificate" issued to Commerce Decisions web server, is a Symantec Class 3 Secure Server. This ensures that the information being communicated between the user's web browser and AWARD is secure.

User Access to the AWARD® System

Access to AWARD® is controlled through users being assigned to roles within AWARD® (see Table 1), and through their username and password. Users are initially created at the Account level, and then assigned to the one or more projects as required.

If a user is not entered at the Account level, they cannot access any part of AWARD®, and by design, cannot be connected to the database. For the conduct of Evaluation Projects, Commerce Decisions support team enter the user's details into AWARD®, and then either they, or the Client's Administrator assign them to the relevant projects.

All access to AWARD® is logged in the AWARD® audit trail, which can be searched to identify when users have logged into AWARD® as well as any actions they undertake e.g. viewing a document. Commerce Decisions also monitors the server access logs, and can provide a report listing the users and the IP addresses they access AWARD® from – providing confirmation that all users are accessing AWARD® from the approved locations.

External access to the AWARD® Database

As noted in the previous section User Access to the AWARD® System, to access AWARD® the user must be assigned at the Account level. If the initial authentication does not occur, the user cannot access AWARD® or gain access to the underpinning database. As illustrated in Figure 3 below, the flow within the system is from the top down into the database. It is not possible to access the database directly.
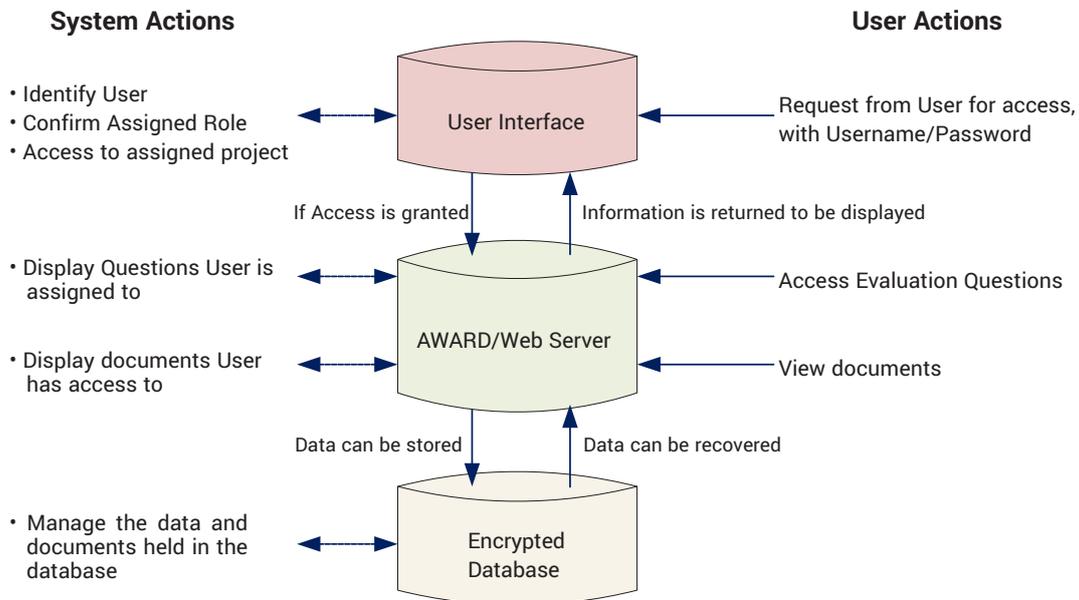
System Actions

User Actions

• Identify User
• Confirm Assigned Role
• Access to assigned project

User Interface

Request from User for access, with Username/Password

If Access is granted

Information is returned to be displayed

• Display Questions User is assigned to

AWARD/Web Server

Access Evaluation Questions

• Display documents User has access to

View documents

Data can be stored

Data can be recovered

• Manage the data and documents held in the database

Encrypted Database

Figure 3: Security Model

All data and documents stored within the database are encrypted, meaning it is not possible to view the data or documents directly in their original format e.g. .doc, .xls, .pdf.

Access to Documents within AWARD®

AWARD® can store and electronically manage all documents relating to an evaluation. It does this by loading the documents into pre-determined Document Groups – as shown in Figure 4 below. When the Questions are created within AWARD®, they are linked to a Document Group or Groups, which in turn restricts users assigned to those Questions to only view or search upon documents in the associated Document Group.
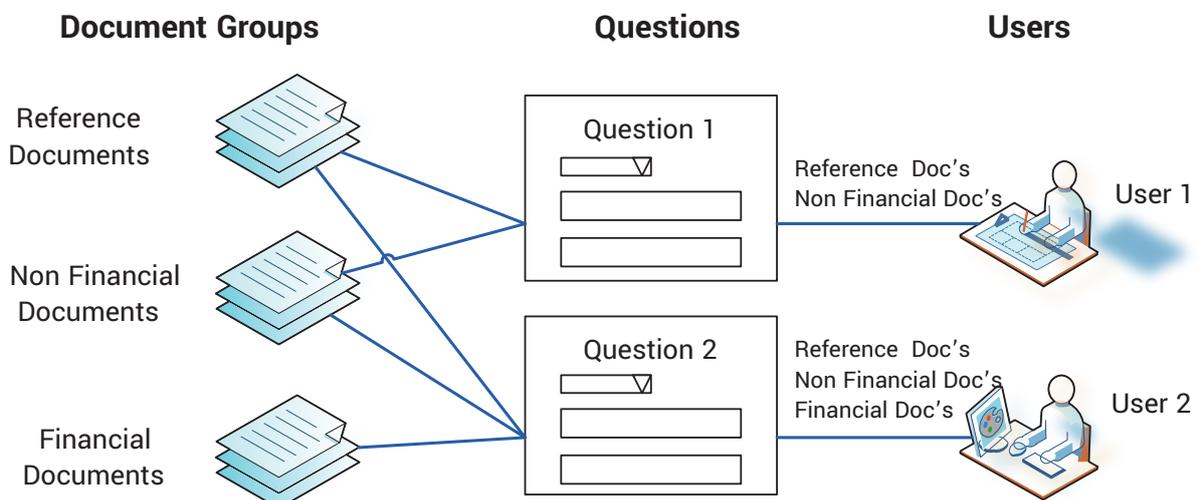
Document Groups

Questions

Users

Reference Documents

Non Financial Documents

Financial Documents

Question 1

Reference Doc's
Non Financial Doc's

User 1

Question 2

Reference Doc's
Non Financial Doc's
Financial Doc's

User 2

Figure 4: **Document Management**

In the example shown in Figure 4, the Financial documents have been separated from the NonFinancial/ Technical documents. This ensures that evaluators can only see the documents relevant or permitted as part of their work.

All access to documents is recorded in the AWARD® audit trail. There are in-built reports within AWARD® to enable an audit report to be created at any time to confirm compliance with the access requirements as stated in the Tender Evaluation Plan.

Access by Commerce Decision Support

Access by Commerce Decisions Support personnel is limited to only those named in the contract documents, as named resources. Any personnel hold at least a BASELINE security clearance.

Access to AWARD® by Commerce Decisions personnel is recorded in the AWARD® audit trail, which can be searched to identify when users have logged into AWARD® as well as any actions they undertake.