



Department of Education and
Early Childhood Development

DEECD ITD Solution Architectural Standards

Release: Final

Document Date: January 2011

Document Version: 2.1

Solution Architecture Office

Information Technology Division

Department of Education Early Childhood Development

Copyright © 2011

This document is the property of the Department of Education and Early Childhood Development who shall retain its copyright. It may not be reproduced or recorded in whole or part in any form or media without the explicit written approval of the Department of Education and Early Childhood Development.

Contents

1	DEECD Standards	3
2	Introduction	4
	2.1 Purpose	4
	2.2 Background	4
	2.3 Scope	4
	2.4 Exceptions	4
	2.5 Assumptions	4
	2.6 References	4
	2.7 Definitions	5
3	Definition of Class	6
4	Application Architecture	6
	4.1 Development Language	6
	4.2 Integrated Development Environment (IDE)	6
	4.3 Software Development Framework	6
	4.4 Application Design	6
	4.5 Development Environment Tools Standards Summary	8
	4.6 Application Transaction Management Standards	8
	4.7 Application Business Intelligence	8
	4.8 Client-Side Presentation Standards	9
	4.9 Web Browser Standards	9
	4.10 Enterprise Portal	9
5	Platforms	9
	5.1 Client Platform	9
	5.2 Web Server	9
	5.3 Application Server	10
	5.4 Load Balancing	10
6	Application Security	10
	6.1 General Security	10
	6.2 Authentication	10
	6.3 Authorisation	10
	6.4 Cryptography	11
	6.5 Auditing, Logging and Alerting	12
	6.6 Data Protection in a Distributed Environment	13
	6.7 Identity Management	13
7	Data and Databases	13
	7.1 Database Management	13
	7.2 Data Transfer Standards	14
8	MS Access Based Solutions	14
9	Infrastructure Server System Architecture	14
	9.1 Client Operating Systems	14
	9.2 Server Operating Systems	15
	9.3 Virtualisation Services	15
	9.4 Server Hardware	15
	9.5 Storage Hardware	15
	9.6 Network Hardware and Services	15
10	Infrastructure Management Tools	16

1 DEECD Standards

Development	Programming Language	Microsoft Visual Basic .NET v9.0			
	Client Presentation Languages	Microsoft ASP.Net (VB.Net)	Microsoft .NET Smart Client	XHTML 1.0 Strict HTML 4.01 CSS 2.1	JavaScript
	Integrated Development Environment	Microsoft Visual Studio .NET 2008	Microsoft Visual Source Safe 2005		
	Software Development Framework	Microsoft.Net Framework v3.5			
Core Application Services	Client Platform	Microsoft Office 2007	Microsoft Office 2003		
	Web Browser Standards	Microsoft Internet Explorer 8.0			
	Enterprise Portal	Microsoft Office SharePoint Services 2007 SP1	Microsoft SharePoint Server 2010	Microsoft Lync Server 2010	
Infrastructure Services	Business Intelligence	Microsoft SQL Server 2008 R2 Reporting Services	Microsoft SQL Server 2008 R2 Analysis Services	Microsoft PerformancePoint Services 2010	
	Web Server	Microsoft Internet Information Server 7.5			
	Application Server	Microsoft IIS 7.5 & .Net 3.5 Framework			
	Identity Management	Microsoft Active Directory	Hyro Idaptive	SAML 2.0	
	Data Management	Microsoft Exchange Server 2010	Microsoft SQL Server 2008 R2		
	Data Transfer Standard	Microsoft SQL Server 2008 R2 Integration Services	Web Services		
	Server Operating System	Microsoft Windows Server 2008 R2			
	Client Operating System	Windows 7	Windows Vista	Windows XP	
Infrastructure	Virtualisation	VMWare	Citrix XenApp 6		
	Server Hardware	IBM X-Series Servers			
	Storage Hardware	SAN			
	Network	Gb Switched Ethernet	Cisco Switch, routers, Firewall	Cisco WAC	
	Management Tools	Microsoft System Center SCCM & SCOM 2007	IBM Director	Back Up Exec	HP BAC

2 Introduction

2.1 Purpose

This document defines the standard technological requirements for ITD application development at DEECD. All technologies use for DEECD application development must fall within the stated standards. Technologies not within the guidelines are implicitly prohibited.

Consult the ITD Solution Architecture Office if advice and/ or assistance are required

2.2 Background

DEECD ITD has standardised on a consistent and organisation-wide approach to application development to ensure that vendors engaged on IT Projects produce applications in-line with departmental standards.

2.3 Scope

This document defines standards which software development teams should conform to when providing solutions for DEECD.

This document covers

- Application Architecture
- Technology Standards including but not limited to n-tier design considerations, development platform, data and database considerations
- Reporting and reporting services

This document does not address detailed design, although recommendations are made across some areas, and should be used in conjunction with other artefacts such as:

- Developer's resource kits
- Technical Architecture
- Security Guidelines
- Infrastructure Standards.
- DEECD Architecture Principles

2.4 Exceptions

There are no exceptions to these standards. Business units with compelling business cases for varying from these standards will be required to submit proposals to the DEECD Enterprise Architecture Board and ITD GM.

2.5 Assumptions

All technologies defined and classified in this document are valid from January 2011 onwards or until a new version of this document is released.

2.6 References

Ref#	Title	Document Id
1	Developers' Resource Kit	http://www.education.vic.gov.au/devreskit .

2.7 Definitions

Acronym/Term	Meaning
BAU	Business as usual
COM	Microsoft Component Object Model
COTS	Commercial Off The Shelf product
DNA	Microsoft Distributed Internet Application Architecture
DEECD	Department of Education and Early Childhood Development
EA	Enterprise Architecture
EAB	Enterprise Architecture Board
GAC	Global Assembly Cache
HTTP	Hypertext Transfer Protocol
ICT	Information Communication Technology
ITD	Information Technology Division of the DEECD
OEM	Original Equipment Manufacturer
NFR	Non-Functional Requirement
SLA	Service Level Agreement
SOA	Service Oriented Architecture
UML	Unified Modeling Language
WSE	Microsoft Web Service Enhancements
WCF	Windows Communication Foundation
XML	Extensible Mark-up Language

3 Definition of Class

This section specifies the terms used in this document.

Class	Definition
DEECD Standard	This is the standard technology for DEECD application development.

4 Application Architecture

4.1 Development Language

VB.Net is the development language for new applications

Class	Language
Standard	Microsoft Visual Basic.Net v9.0

4.2 Integrated Development Environment (IDE)

The current development environment is Microsoft Visual Studio.Net 2008.

Product
Microsoft Visual Studio .NET 2008 (only VB.Net)
Microsoft Visual SourceSafe 2005

4.3 Software Development Framework

Microsoft .Net Framework v3.5 is the software development framework.

Product
Microsoft.Net Framework v3.5

4.4 Application Design

DEECD applications are to be developed with an n-tier design.

Design	Description
N-Tier	The presentation, business and data tiers all completely separated, having each tier designed to transparently talk to subsequent tiers whether they are hosted locally or remotely. The ability of host separation allows scalability.

The recommended guideline for software solution would include, but is not limited to, the following software layers.

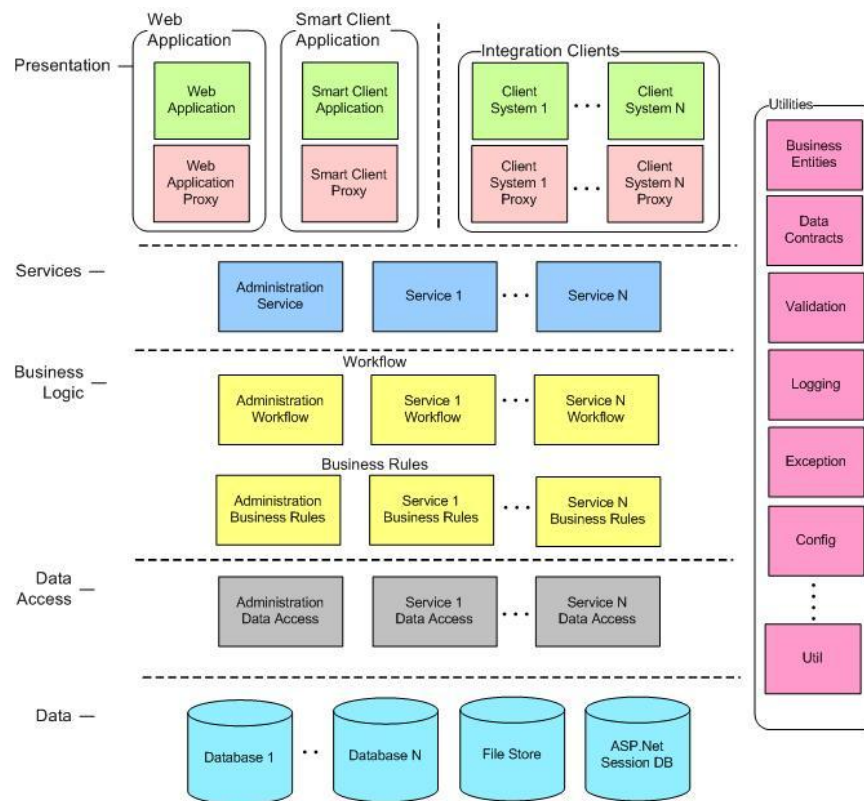


Figure 1 - Recommended N-tier Application Architecture

The structural representation of the solution abides by the architectural principals of a layered application. Application elements are separated into distinct layers of components to enable high coherence and low coupling.

- **Presentation:** This layer is the location for any user interface related code. The presentation of the system can be in the form different types of clients with the need of consuming the application services.
- **Service Agents:** This layer hides from the client application the details required to successfully invoke the service or perform remote service calls.
- **Service Layer:** This layer encapsulates the data contracts, or business entities, and services which are exposed for the vertical partitions. To the extent possible this layer must isolate from the rest of the system any service communication concerns such as fault management and data contract definitions.
- **Business Logic:** Components of the system which define the business logic boundaries such as workflow, validation and business rules. The diagram above encourages the separation of workflow and business rules, based on the assumption that business rules are more likely to have frequent changes in comparison to business processes.
- **Data Access:** Components solely used for the purpose of accessing data from the system data stores. This layer abstracts the semantics of the underlying data store and data access technology providing a simple interface for retrieving and performing operations on data.
- **Data:** This layers houses any databases and persistent storage participants such as files.
- **Utilities:** The components in this partition are components which are common across two or more layers of the entire system and are therefore represented as a vertical slice of the architecture.

4.5 Development Environment Tools Standards Summary

Product
Enterprise Libraries 5.0
Web Client Software Factory (WCSF)
Web Service Software Factory Modelling Edition 2008
Microsoft Team Foundation Server

4.6 Application Transaction Management Standards

Transactions are to be used for any operation where the state of the systems is expected to alter after the execution of the request such as the creation of a database record. Operations where data is only presented to the user without the need of modifications do not need the use of a transaction.

The selection criteria for using transactions is tightly coupled with the architecture of the components involved within the business operation. As per the above criteria, transaction should be used throughout the system. However if a business operation(s) requires a long running transaction – i.e. expected to take longer than a minute – and the user may experience a long delay or a request failure; transactions should be implemented by separating the process or workflow steps into individual transactional operations. A transactional queue is a good candidate for such an implementation. Such separation allows the operation to be enclosed within transactions without resulting in unwanted user experiences.

Explicit management of transactions is labour intensive and error prone. .Net 2.0 introduced a new model for transaction management which greatly simplifies the effort and implementation for the developers. Application developers should consider the use of the Transaction Scope feature of .Net

4.7 Application Business Intelligence

Report data may be printed, stored locally, emailed, transmitted by a notification channel (SMS) or may be the trigger of other business processes via a messaging or bulk data transfer interface. Furthermore, report information may also be used as part of an enterprise reporting facility such as a data warehouse and may therefore need to be injected into other systems.

Reports may be produced using specific functionality designed into the application code or by the use of a generic report generation program or service. The report generator can be called from within the application using specific service calls (APIs) or manually by extracting the data in an agreed format (e.g. XML) and submitting it to the report generator.

Applications developed internally using SQL Server as a backend database should use SQL Server Reporting Services (SSRS) as the means of delivering such information.

Technology
Microsoft SQL Server Reporting Services 2008 R2
Microsoft SQL Server Analysis Services 2008 R2

4.8 Client-Side Presentation Standards

Product	Comments
HTML 4.01 XHTML 1.0 CSS 2.1 Java Script	Although JavaScript can be used, the site must be functional with JavaScript turned off. For more details refer to: http://www.education.vic.gov.au/devreskit/webdev/javascript.htm

4.9 Web Browser Standards

Product
Internet Explorer 8.0

4.10 Enterprise Portal

The DEECD enterprise portal is currently based on Microsoft Office SharePoint Services 2007; however migration to Microsoft SharePoint 2010 is planned during 2011.

Product
Microsoft SharePoint Server 2010
Microsoft Office SharePoint Services 2007 SP1

5 Platforms

5.1 Client Platform

Product
Microsoft Office 2003
Microsoft Office 2007

5.2 Web Server

Web servers serve up content to the client web browser.

Product
Microsoft IIS v7.5

5.3 Application Server

Application servers perform the processing logic in most web applications. These can either be hosted on the same box as the web server or they can be hosted separately.

Product
Microsoft IIS 7.5 /.Net 3.5 Framework

5.4 Load Balancing

Microsoft Forefront Threat Management Gateway terminates HTTPS or SSL Certificates and securely publishes web content across multiple web farms on hosts. Contact EduMail Services telephone: 96372956 for additional information.

Product
Microsoft Forefront Threat Management Gateway (TMG) 2010

6 Application Security

6.1 General Security

DEECD has a published set of guidelines on ICT Security Standards. Contact Manager, Risk Management telephone: 96373856 on ICT Security Policy.

6.2 Authentication

Authentication can be defined as the process of verifying the source (Identity) of engagement for a system – a source being a user or another system. DEECD application users must be protected against threats such as:

- Identity high-jacking
- Password cracking

DEECD uses an LDAP compliant directory as its source of user data for network level authentication. Currently this directory is Microsoft Active Directory.

All applications developed for the DEECD should use this directory as its source of user authentication.

All applications using a database will use a dedicated application account to authenticate against the database server.

6.3 Authorisation

Authorisation is the process of granting access to a network resource based on the already established identity. Authorisation ensures that the authenticated user is given the correct privileges to the correct resources accessible by the system. The resources each user has access to will depend on their role membership.

DEECD user roles must have appropriate access to confidential data as well as system operations. A control mechanism must exist within the application to prevent:

- Escalation of privileges
- Access to restricted system areas and or features
- Tampering with data

Authorisation methods should be based on the security principle of ‘Least Privilege’ where architects and team leads of the system are encouraged to design the application to allow the code executing under an authenticated identity to function with the minimum set of user rights required to successfully complete the intended operation. This creates a ‘Secure by Default’ system user configuration.

Solutions must also provide a user authorisation matrix as part of the documentation. This document facilitates the solution auditing and configuration.

Role Authorisation Matrix	User Type 1	User Type 2	User Type 3	User Type N
System Scope 1				
Validate User	A	A	A	A
Verify Role	A	A	A	A
Write Audit Log	A	A	D	A
Write Transaction Status	A	A	D	A
Write Access Log	A	A	D	A
Write Change Log	A	A	D	A
System Scope 2				
Data Import	A	A	D	D
Update education record	A	D	D	D
Perform provider Search	A	A	D	D
Add Record	D	D	A	A
System Scope 3				
Generate Audit Log Report	A	D	A	D
Generate Access and Change Log Report	A	D	A	D
Generate Student Statistics Report	A	D	D	D
A = Accept				
D = Deny				

Figure 2 Authorisation Matrix

The diagram above illustrates a sample authorisation matrix documented required by the solution.

6.4 Cryptography

The DEECD has a published set of clear guidelines on what, where and how cryptography should be used within developed software, databases and the servers hosting these systems. This document is known as the ‘ICT Security Standard – Using Cryptography to protect information’.

The following points highlight some of the standards used within the DEECD environment:

- Cryptography must be used for sensitive information which is either:
 - Kept on persistent storage
 - Transmitted over the network
- Code signing of all DLL’s and Executables published on a public facing website (including those that are visible to schools) must be code-signed by the DEECD so that the receiver knows they come from a trusted source.

- Message layer encryption for public facing websites should use X.509 certificates and be combined with SSL 128bit encryption. The DEECD uses trusted certificate authority such as Thawte (www.thawte.com) and/ or DigiCert for acquiring SSL certificates.
- Sensitive data (including data on backup media, in logs, exchange of information in from and out to external systems) must be rendered into unreadable form anywhere it is stored. Different approaches can be applied to do:
 - One-way hashes
 - Truncation
 - Index tokens with PADs (with the PAD being securely stored)
 - Strong cryptography such as Triple DES 128-bit should be used as a minimum although AES 256-bit with associated key-management process and procedures is preferred
- The Architecture team must approve any different approaches proposed by application development teams
- If a development team chooses to encrypt data using a key-management technique, the encryption keys must be protected against both disclosure and misuse
- Key-management processes and procedures must be fully documented, including:
 - Generation of strong keys
 - Secure key distribution
 - Secure key storage
 - Periodic key changes
 - Destruction of old keys
 - Split knowledge
- Dual control of keys (this requires two or three people knowing only their part of the key and the whole key only being constructed using all of their keys).

6.5 Auditing, Logging and Alerting

The following requirements concern auditing, logging and alerting:

- All applications must be designed in such a way that it will record and retain the auditing logs for possible evidence in the case of security incident.
- The application and infrastructure must have an appropriate logging, auditing and alerting mechanism in place
- Auditing and logging must take place across all the tiers in the delivered application
- Security systems and processes must be regularly tested
- Any user operation must be auditable through the system

Application developers should consider the use of the Microsoft Logging Application Block, part of the Microsoft Enterprise Libraries, as part of the implementation. See References Section 2.6 above.

6.6 Data Protection in a Distributed Environment

DEECD has sensitive data in its production systems. Protecting, securing and maintaining the integrity and confidentiality of sensitive data has the highest priority within DEECD in order to adhere to legal standards and audit requirements.

DEECD has many environments such as development, system test, user acceptance testing and production. Data must be protected in all of these environments.

The following points need to be considered when considering the use of sensitive data in any environment:

- Protection of Real-Time Data: The information used in testing is generally used by various groups at DEECD. These include groups such as the DEECD internal testing team, outsourced testers and consultants from various outsourcing organisations. Availability of information to various groups increases the likelihood of compliance violation. The Architecture team suggests that you protect and scramble data early in the test cycle.
- Data Creation: The data for the test cycle must be created by the application owner. The data must be realistic in order to conduct proper testing; attempting to obtain data from production and scrambling it may result in too many failed tests.
- Data Obfuscation: Data obfuscation can cause serious problems such as loss of natural data distribution. An obfuscated system may end up behaving quite differently from a clear-text system. Clustering factors, data lengths and distribution of values may all be quite different from the real system.
- Important Data Fields: Important data is often referenced by many fields. Care must be taken when altering the key fields; for instance, where the name field of a student is scrambled but is also referenced in a comments section.
- System Outputs: Where data has been scrambled, you must also consider system outputs very carefully, such as printouts, faxes, e-mails etc. This may result in compliance violation.
- Data sensitivity: Avoid using production data in non production environments

6.7 Identity Management

Product
Microsoft Active Directory
Hyro Idaptive – Hyro proprietary Identity Access Tool
SAML 2.0

7 Data and Databases

7.1 Database Management

Microsoft SQL Server 2008 is the database management system for new applications.

Product
Microsoft SQL Server 2008 R2

7.2 Data Transfer Standards

DEECD has the following standards for data transfer.

Technology
SQL Server Integration Services (SSIS) 2008 R2
Web Services

8 MS Access Based Solutions

Externally developed MS Access-based applications are not permitted within the DEECD environment.

Applications written in MS Access should only be used to meet short-term needs and have:

- No access to sensitive data
- No interface to external applications
- No more than 3 concurrent users
- A low volume of transactions
- No scalability requirements
- No security requirements
- No audit trail requirements
- No general compliance requirements

This technology is not suitable for applications containing sensitive and important information.

The use of this technology (or enhancements to existing MS Access-based applications if applicable) requires appropriate approval.

9 Infrastructure Server System Architecture

9.1 Client Operating Systems

Product
Microsoft Windows 7
Microsoft Windows Vista
Microsoft Windows XP

9.2 Server Operating Systems

The operating systems at DEECD is Microsoft Windows 2008

Product
Microsoft Windows Server 2008 R2

9.3 Virtualisation Services

VMware is the virtualisation services.

Product
VMware
Citrix XenApp 6

9.4 Server Hardware

IBM X-Series Server is the Server hardware used in DEECD

Product
IBM X-Series Servers

9.5 Storage Hardware

SAN is the DEECD Storage Hardware of choice.

Product
SAN

9.6 Network Hardware and Services

The network hardware and services are:

Product
Gigabit Switched Ethernet network
Cisco switching
Routing and firewall equipment

10 Infrastructure Management Tools

The current monitoring tools in DEECD are as listed:

Product
Microsoft System Center 2007 Operations Manager and Configuration Manager
IBM Director
Backup Exec
HP BAC