



# Financial Management System (FMS)

## Technical Architecture Design

Department of Education  
Student Financial Assistance

May 3, 2001

---

# Contents

Background.....	<u>11</u>
Phase III Technical Design Considerations.....	<u>87</u>
FMS Environments.....	<u>1412</u>
Oracle Software Inventory .....	<u>1614</u>
Back-end Interface Requirements.....	<u>1715</u>
Guaranty Agency Migrations.....	<u>1917</u>
Future Project Considerations.....	<u>2018</u>

---

## **Background**

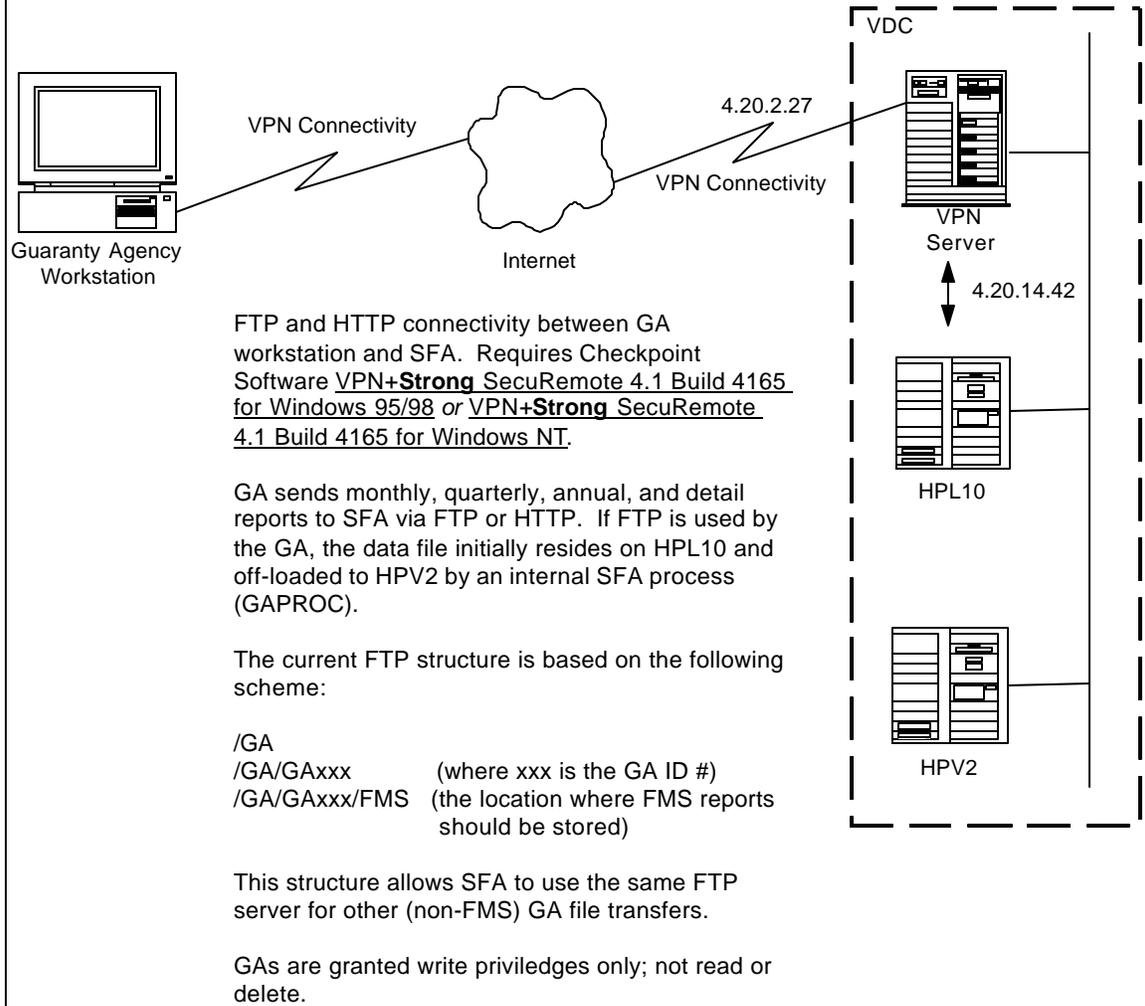
### Phase II Architecture

The Financial Management System (FMS) phase II architecture allows Guaranty Agencies (GAs) to submit monthly, quarterly, and annual reports to the Department of Education, Office of Student Financial Assistance (SFA) via web-accessible (Java) screens or files transferred via FTP. The FTP and web servers required for GA submissions are located at the VDC; GA users are considered external users to this facility. Therefore, VDC access requires authentication via Virtual Private Network (VPN) server.

SFA's VPN architecture is designed to provide access by individual workstations with direct Internet connections; it is not designed for access from workstations with Internet access from an internal private network (e.g., via proxy server). Although this limitation has proven cumbersome for the GA community, it can easily be overcome through dial-up Internet access (including the use of "Free Internet Service Providers").

FMS phase II architecture employs VPN, FTP, and Web servers for external user processing. Authentication from the VPN server allows the external user to access the FTP and/or Web server. Each server authenticates users from separate user/password files, each of which is controlled by separate groups within the SFA environment (e.g., VPN and FTP are managed by CSC and Web access to the FMS application is managed by FMS team).

## Phase II GA Processing



### Phase III Architecture

Although currently the GA user population is relatively small (~200 individuals), there have been significant challenges and some delays associated with establishing userid/passwords for all GA users and system components (i.e. VPN and FTP). Under FMS phase III, we expect an additional 110 to 125 external users for the LEAPP rollout. This issue will be exacerbated with later Phase III and IV implementations, when additional users will be authorized. The current estimate is approximately: 10,000 organizations and 10,000 – 15,000 users. The proposed phase III architecture has been designed to provide the foundation and flexibility to support changing requirements, given some application design

decisions (e.g. COD, schools, etc...) have not been made. Therefore, this architecture may need to change to accommodate those application design changes.

The intent of this architecture design is to:

- provide the flexibility to support the current and anticipated future user population (although additional machines may be required),
- provide a migration path away from reliance on externally-maintained VPN/FTP systems, and
- eliminate the need for VPN/FTP userid coordination.

Phase III interfaces will take full advantage of FMS' built-in COTS security functions provided in the Oracle Financials software. The Technical Architecture team, software development lead, and Oracle technical representative agree that all custom extensions and interfaces will rely on FMS' built-in COTS security authentication and validation technology. In other words, custom Oracle security packages, procedures, and/or programs will not be developed under Phase III.

The FMS Technical Architecture team evaluated several possible configurations to meet Phase III requirements, particularly how to architect and configure an external web server, including:

- Forms coded in native HTML, using CGI, Java, or JavaScript, Java Server Pages and ODBC,
- Forms coded in above, stored in the database, and served from Oracle Web Application Server accessible from the Internet
- Oracle Forms developed along Oracle Applications Development Guidelines, but placed on a server accessible via the Internet.
- Forms developed using application development tools other than Oracle, such as Visual Age for Java (IBM), Cold Fusion, etc.

Meetings were held between the Technical Architecture team, Development team lead, FMS developers, and Oracle representatives to discuss alternative methods for Phase III development. Some of the potential solutions were rejected due to non-conformance with SFA technical architecture and

software development standards. After meeting with the FMS software development team lead and Oracle technical representatives, the FMS Technical Architecture team decided to test the use of a second web server/form server for external user access. With this option software development would continue using Oracle Forms 4.5 (the current, approved software development tool). A proof-of-concept test was conducted and validates this configuration's viability.

### External User Access Security Considerations

SFA and the FMS team understand the serious responsibilities in systems design to protect computer system resources from malicious acts and maintain both data integrity and privacy. The FMS project team presents an architecture that complies with SFA security rules based on federal government security policies and regulations. In addition, this architecture has been coordinated with SFA security representatives and incorporated into the SFA FMS Security Plan.

Generally, computer systems are at risk when a threat can take advantage of a vulnerability to cause harm. A threat is any circumstance or event with the potential to cause harm to an organization through the disclosure, modification, or destruction of information, or by the denial of services. Organizations and application systems have different levels of sensitivity to risk, and they should develop and adopt security policies that reflect their particular sensitivities. [Information Security and the World Wide Web, National Institute of Standards and Technology (NIST), Information Technology Laboratory (ITL) 98-02]

Organizations that support external user access typically place their servers outside the organization's firewall. The publicly accessible computer server is potentially a target for vandalism and break-ins, as documented by many well-publicized incidents over the past few years. Attackers exploited weaknesses in the base operating systems of the computer server, and broke into the sites with apparent ease. Public embarrassment to the organization is one consequence to an attack; if the attackers successfully place false data into the system's accounting database, then the consequences will be more severe.

General Accounting Office (GAO) audits of the Department (and other departments/agencies) identify weaknesses in

security management as well as the requirement in restricting data and applications access (emphasis added):

Evaluations published since July 1999 continue to show that federal computer systems are riddled with weaknesses that continue to put critical operations and assets at risk...they placed an enormous amount of highly sensitive data—much of it pertaining to individual taxpayers and beneficiaries—at risk of inappropriate disclosure.... *Controls over access to...system software are essential in providing reasonable assurance that operating system-based security controls are not compromised and that the system will not be impaired.* If controls in this area are inadequate, unauthorized individuals might use system software to circumvent security controls to read, modify, or delete critical or sensitive information and programs.... [Computer Security: Critical Federal Operations and Assets Remain at Risk, 9/11/2000]

The information systems weaknesses highlight some of the computer security vulnerabilities...*Information systems control weaknesses increase the risk of unauthorized access or disruption in services and make Education's sensitive grant and loan data vulnerable to inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction, which could occur without being detected...*[Financial Management Challenges Remain at the Department of Education, 9/19/2000]

Additionally, the Office of Management and Budget (OMB) defines government-wide information resources management in Circular A-130, of which the need to limit external user access is required (emphasis added):

"Adequate security" is defined as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information." This definition explicitly emphasizes the risk-based policy for cost-effective security established by the Computer Security Act.... *The development of rules for a system must take into consideration the needs of all parties who use the system. Rules should be as stringent as necessary to provide adequate security.* Therefore, the acceptable level of risk for the system must be established and should form the basis for determining the rules....

Public Access Controls. Permitting public access to a Federal application is an important method of improving information exchange with the public. At the same time, it introduces risks to the Federal application. *To mitigate these risks, additional controls should be in place as appropriate. These controls are in addition to controls such as "firewalls" that are put in place for security of the general support system....*

Official records need to be protected against loss or alteration. Official records in electronic form are particularly susceptible since they can be relatively easy to change or destroy. *Therefore, official records should be segregated from information made directly accessible to the public.* There are different ways to segregate records. Some agencies and organizations are creating dedicated information dissemination systems (such as bulletin boards or World Wide Web servers) to support this function. These systems can be on the outside of secure gateways, which protect internal agency records from outside access....

*In order to secure applications that allow direct public access, conventional techniques such as least privilege (limiting the processing capability as well as access to data) and integrity assurances (such as checking for viruses, clearly labeling the age of data, or periodically spot checking data) should also be used....*

To provide for adequate security, specific steps to protect public access systems are proposed in NIST's Information Technology Laboratory (ITL) bulletins and Computer Security Resource Center (CSRC) publications (emphasis added):

Web servers are vulnerable to threats, especially to malicious threats. Web servers can be attacked directly, or they can be used as jumping off points to attack an organization's internal networks. *Organizations should examine the underlying operating system of their Web server, the Web server software, server scripts and other software for vulnerabilities.* [Information Security and the World Wide Web, ITL, 98-02]

Techniques to Secure Web Servers: The most common methods for protecting Web servers include:

- Removal of unnecessary software,
- Detection of attacks upon a Web server,
- Correction of flaws in remaining software,
- Restriction of an attacker's actions once a part of a Web server is compromised, and
- Protection of the rest of the network if a Web server is compromised. [ITL Bulletin September 1999]

Finally, the FMS technical architecture team has addressed these guidelines and security controls (to reduce external web server vulnerabilities and risks) from an architecture view point by answering the following questions:

1. What specific forms, functions, processes, and reports are required for external access?
2. Who shall have access to these components?

3. From where shall external access be granted?
4. How can we mitigate unauthorized access?

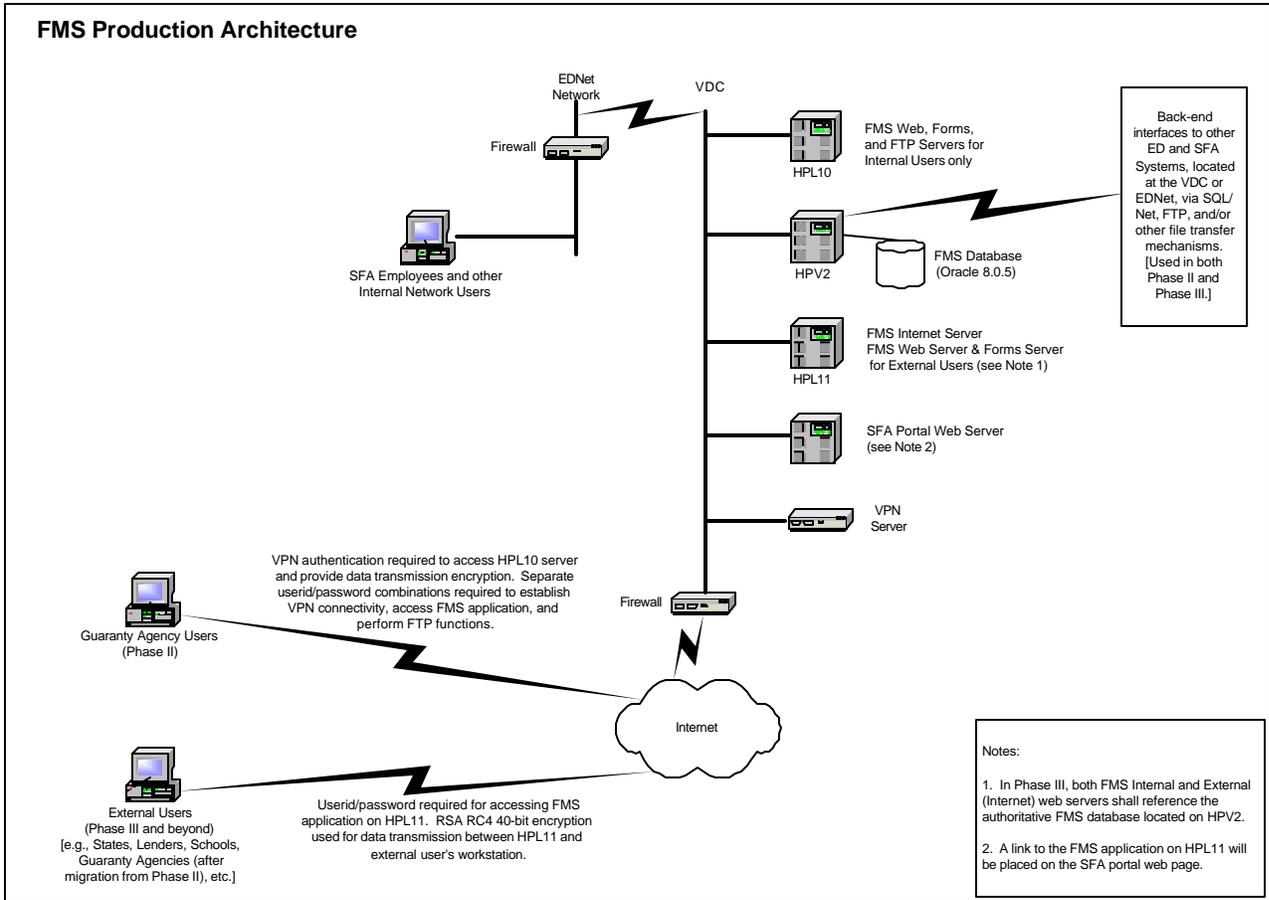
The FMS team is confident that this technical architecture complies with federal, Department of Education and SFA (including their respective CIO organizations) security policies to allow authorized external users to perform specific and limited FMS functionality. Although the potential exists for malicious acts on the external server, the architecture includes provisions that mitigate potential damage to the FMS system.

---

## Phase III Technical Design Considerations

In consideration of the A-130 definition of adequate security, and to mitigate unauthorized access, a second Oracle web/form server configuration will be installed for external user processing. This external web/form server will contain only those processes, forms, and functions that are needed by the external user community. This second external Oracle web/form server configuration will not contain any functions limited to internal users only (e.g., SFA employees that perform General Ledger functions, authorize payments, etc.). In this manner, unauthorized access to FMS data from the Internet is restricted to only the data normally available to external users.

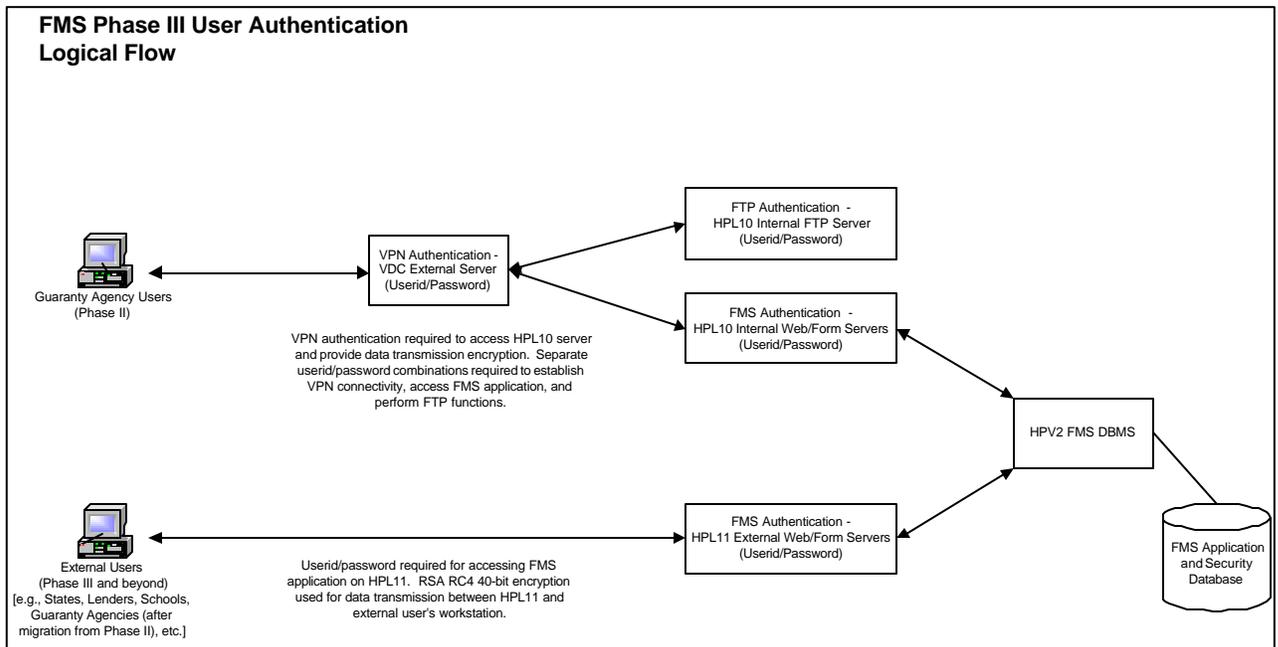
The proposed FMS phase III architecture (shown on the next page) eliminates VPN and FTP servers for new Phase III interfaces. The Phase III design provides FMS with the opportunity to migrate GAs off the VPN solution by installing the GA software on the second (external-access) web server. Installation on the second web server does not require removal of the same software from the internal-use web server; the GA will have the capability to continue using the VPN solution, although we recommend they be migrated off as soon as reasonably possible to completely eliminate the use of VPN and FTP. [Note that VPN usage requires SFA CIO authorization. Further, SFA CIO may replace the current VPN product with a different solution.]



The second web server configuration will also reside at the Virtual Data Center (VDC) on an HP L-class server (HPL11), with an Internet-accessible IP address. This web/forms server configuration will contain the minimal FMS COTS software to perform security authentication, report processing, and other functions which external user interfaces would require. Additionally, intrusion detection software (Tripwire) will be loaded on HPL11 based on SFA CIO security standards.

The second Oracle web/form server for external user access (located on HPL11) will maintain data in the authoritative FMS database located on HPV2 and requires opening the data transmission ports between HPL11 and HPV2.

Internal users will not be able to access FMS from the external web/form server. Internal users that require FMS access via the Internet will need to obtain VPN access, EDNet dial-in connectivity, or other ED/SFA-provided mechanism that allows data communications to the internal FMS web/form server.



A security vulnerability that exists in many application systems (including FMS) is that authentication is limited to userid/password combinations only. An unauthorized person who masquerades as an authorized user will assume the role(s) and authority(ies) granted to the authorized user. To mitigate unauthorized access from the Internet, the external web/form server will only be able to process those functions allowed by external users. However, because reporting and other concurrent processes are performed by Oracle common functions, an unauthorized person masquerading as an internal SFA employee may be able to view “Internal Use Only” reports and/or cancel processes invoked by the SFA employee.

To this end we propose to limit concurrent processing and report viewing by extending the Oracle security database to identify the application server (internal, external) the user is authorized to access. This effort includes:

1. Modifying the Oracle Applications Sign-on Screen;
2. Creating a data table to identify the application server a user is authorized to access;
3. Creating a table to log successful and unsuccessful sign-ons;
4. Creating an Oracle Forms screen to maintain the tables mentioned above; and

5. Creating one or two reports to present data from the tables created in steps 2 and 3.

The extension can be patched and upgraded with minimal maintenance.

Phase III external users will be provided the capability to connect to an SFA web server directly (i.e. without first having to connect to the VPN server). Additionally, because the current VPN solution is not required for phase III external users under the proposed architecture, external users may access FMS from anywhere via the Internet, regardless of the external user's private IP configuration or use of a proxy servers. This allows FMS to avoid the biggest challenges faced implementing Phase II.

The proposed architecture also allows the FMS application to control access from within its security subsystem, which has already been approved by SFA. The FMS security database contains authorized user records for both internal and external FMS functions. This is one of the primary advantages of using packaged software. The FMS project team will maintain this user access database since FMS has the responsibility of approving and granting user access to the application.

External users will access FMS via hyperlinks placed on the SFA channel home pages. The first group in Phase III are limited to states/territories associated in the Financial Partners' home page. Additional groups may use Schools' and other channel home pages.

Additionally, external users can access FMS by invoking <http://fms.sfa.ed.gov> from their computer's web browser. This link will invoke html to invoke the FMS logon screen (e.g., [http://fms.sfa.ed.gov:8000/PROD\\_j.htm](http://fms.sfa.ed.gov:8000/PROD_j.htm)). Similar to external user recommendations under Phase II, external users under Phase III will need to ensure that data traffic can pass freely between their local network and the external FMS server. This ensures that change(s) to port numbers in the FMS server configuration will not adversely affect the external user community.

Oracle Forms 4.5 is currently planned to be used for Phase III Oracle Forms extensions and modifications. (At some point, depending on SFA enterprise IT standards and FMS' longer-term requirements, this may change.) Interfaces are planned for development using PL/SQL. This offers several advantages:

- Oracle Forms 4.5 was used for Phase II development.
- FMS software developers on staff are experienced with Oracle Forms 4.5.
- Oracle Forms 4.5 presents forms as Java applets to client workstations, meeting ED and SFA standards for software development.
- Forms developed under Oracle Forms 4.5 integrate directly with FMS COTS common functions such as report processing, security, etc.

Use of Oracle Forms would still require Oracle's J-Initiator plug-in to be installed on client workstations, as it was in Phase II. The first time the user signs-on to FMS, the application automatically detects the need for the J-Initiator plug-in and the user is prompted throughout the download process.

The web server for external users will perform data transfer to/from client workstations through RSA RC4 40 bit encryption. RC4 is a stream cipher designed by Rivest for RSA Security. It is designed to encrypt data using variable key-size data streams with byte-oriented operations. The RC4 algorithm is based on the use of a random permutation. RSA Security analysis concluded that "...the period of the cipher is overwhelmingly likely to be greater than  $10^{100}$ . Eight to sixteen machine operations are required per output byte, and the cipher can be expected to run very quickly in software." It is used to secure data communications through data encryption to and from secure web sites using the SSL protocol. Both server configurations will contain exactly the same security functionality provided by the COTS software.

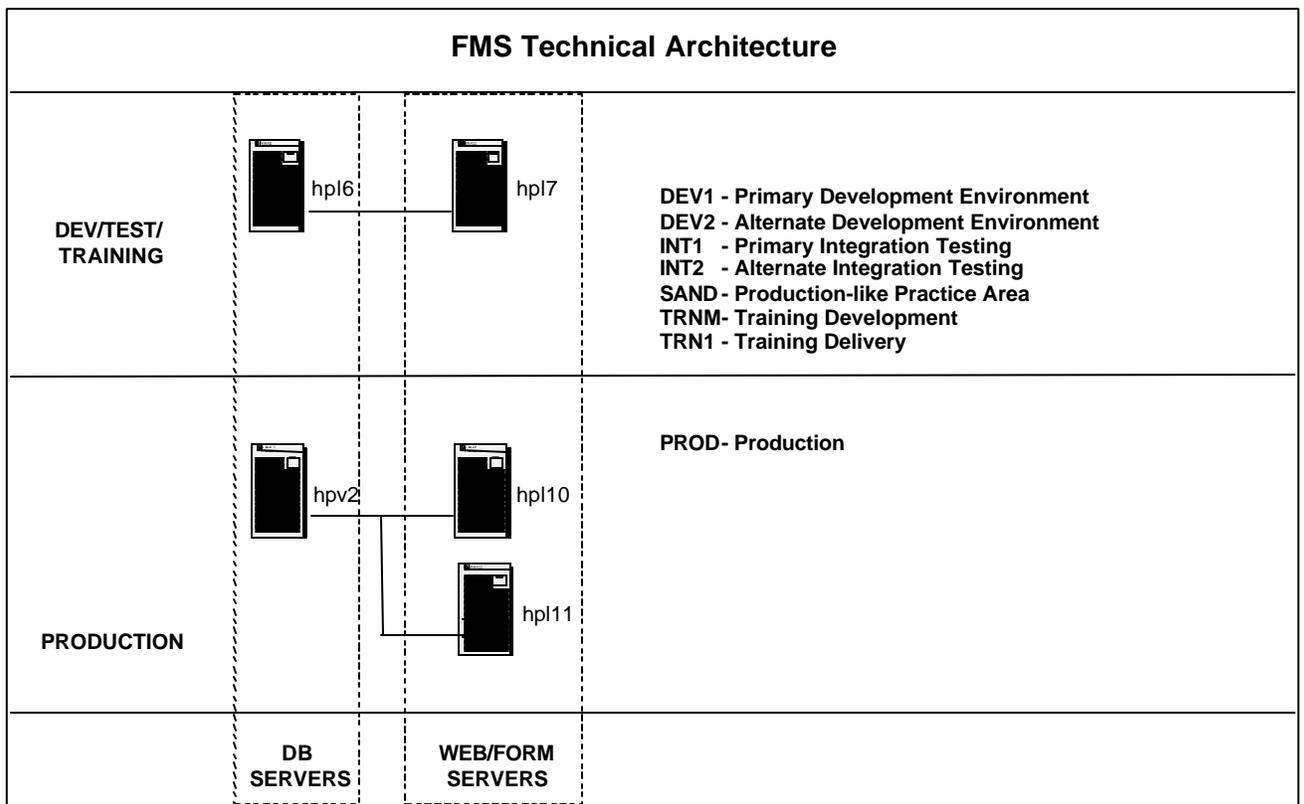
SFA CIO is implementing a Lightweight Directory Access Protocol (LDAP) server to maintain user authentications and authorizations. IF FMS decides to replace the current security database and utilize LDAP, security functions within the FMS COTS software would need to be changed in both the internal and external web/form servers.

The SFA Internet web server may also be used to provide file transfers. By designing a custom form to perform HTTP file transfer, the web server performs the same functions as an FTP server. Once in place, this interface will be easier for the external user:

- External users will not have to perform a separate logon to the FTP server.
- File transfer to the appropriate subdirectory will be performed without user intervention.

## FMS Environments

The following instances are planned for FMS Phase III development, testing, training, production and support. These instances are based on requirements and anticipated needs, as provided by the FMS project team leads. The current FMS hardware (e.g. computers, number of CPUs, CPU speed, memory) configuration is based on information and requirements obtained during Phases I and II. The FMS Technical Architecture Team is currently reviewing the need for these instances with the objective of reducing both the number of instances planned and the number of servers required to support this effort.



## FMS Port Assignments

<b>Instance Names</b>	<b>RDBMS</b>	<b>RPC</b>	<b>UDP</b>	<b>Admin</b>	<b>Web</b>	<b>Forms</b>
<b>Logical</b>	<b>hpl6</b>		<b>hpl7</b>			
TRNM	1581	1582	2652	8893	8700	9700
TRN1	1583	1584	2254	8896	8701	9701
DEV1	1545	1546	2255	8895	8202	9202
DEV2	1547	1548	2256	8897	8203	9203
INT1	1549	1550	2257	8898	8204	9204
INT2	1553	1554	2258	8899	8205	9205
SAND	1557	1558	2260	8890	8207	9207
	<b>hpl8</b>		<b>hpl9</b>			
	<b>hpl9</b>		<b>hpl10</b>			
PROD	1521	1522	2649	8888	8000	9000
			<b>hpl11</b>			
			2649	8888	8000	9000

Database Server Port Types: RDBMS, RPC (hpl6 and hpl8)

Application Server Port Types: UDP, Admin, Web, Forms (hpl7)

Similar to Phase II, external users under Phase III will need to ensure that data traffic can pass freely between their local network and the external FMS server. This ensures that change(s) to port numbers in the FMS server configuration will not adversely affect the external user community.

## Oracle Software Inventory

Component	Version Information <sup>1</sup>	Installation Tier
<b>Operating System</b>	HP-UX Version 11.0 64-bit	Data and Application Server
<b>Compilers for HP-UX</b>	C/C++	Data Server
<b>Oracle Applications</b> <ul style="list-style-type: none"> <li>• Oracle General Ledger</li> <li>• Oracle Payables</li> <li>• Oracle Receivable</li> <li>• Oracle Assets</li> </ul>	Release 11.0.3	Application Server
<b>Oracle Public Sector Applications</b> <ul style="list-style-type: none"> <li>• Oracle Public Sector General Ledger</li> <li>• Oracle Public Sector Payables</li> <li>• Oracle Public Sector Receivables</li> </ul>	Version 3.3 for Release 11.0.3 of Oracle Applications	Application Server
<b>Oracle U.S. Federal Financials</b> <ul style="list-style-type: none"> <li>• Oracle U.S. Federal General Ledger</li> <li>• Oracle U.S. Federal Payables</li> <li>• Oracle U.S. Federal Receivables</li> </ul>	Version 3.3 for Release 11.0.3 of Oracle Applications	Application Server
<b>Tutor</b>	Version 11.0	Client
<b>Oracle RDBMS (Database)</b>	Version 8.0.5	Data Server
<b>Oracle Developer Server 2000</b> <ul style="list-style-type: none"> <li>• Oracle Forms</li> <li>• Oracle Reports</li> </ul>	Version 1.6.1 Version 4.5.10 Version 2.5.7	Client
<b>Oracle Web/Application Server</b>	Version 3.0.2	Application Server (Standard Export Edition)
<b>Oracle Discoverer</b>	Version 3.1.36	Database Server and Client
<b>Java-Enabled Browser<sup>2</sup></b>	Depends on Browser	Client
<b>Oracle Applications Desktop Integrator</b>	Version 6	Client

<sup>1</sup> These version numbers represent the software versions that are available and compatible at March 8, 2000.

<sup>2</sup> Either Microsoft Internet Explorer or Netscape can be used.

### Additional Software Installed

Additional software installed includes:

- Rational TestManager 2001 (Stress Testing) 2001, Version 2001.03.00.

## Back-end Interface Requirements

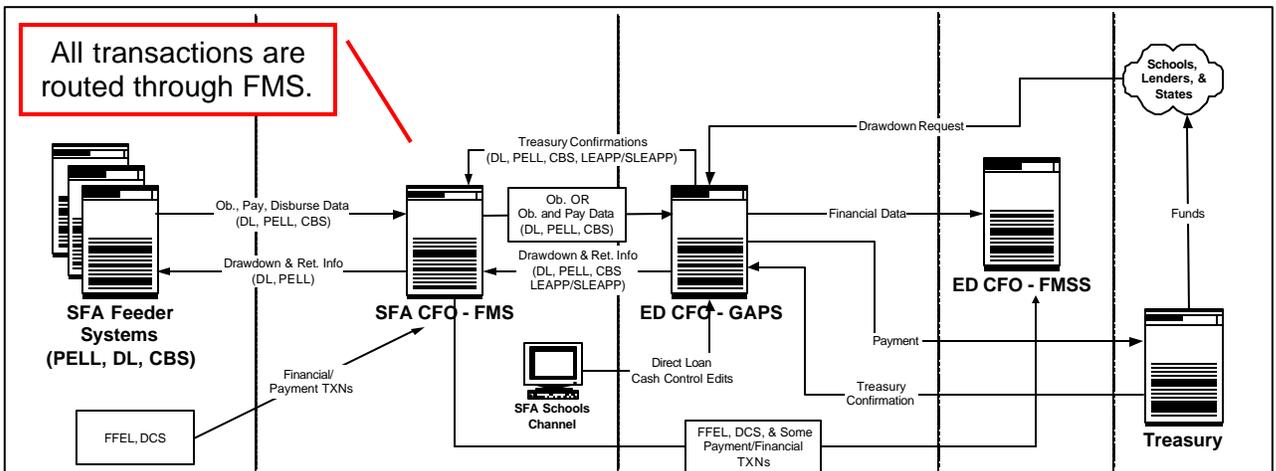
Current production (Phase II) external system interfaces are provided via SQL/Net and FTP. FMS does not invoke, call and/or link directly or indirectly to other systems' application code. Interfaces are back-end data transfer only.

The proposed Phase III interfaces will be performed in a similar manner using SQL/Net, FTP (or other file transfer mechanism) and for back-end data transfer only.

FMS Phase III is expected to interface with the following systems:

- Campus-Based Feeder System
- Debt Collection System
- Direct Loan Origination
- Direct Loan Servicing
- Direct Loan Consolidation
- FFEL Lenders
- Pell RFMS
- LEAPP/SLEAPP (program only)
- GAPS

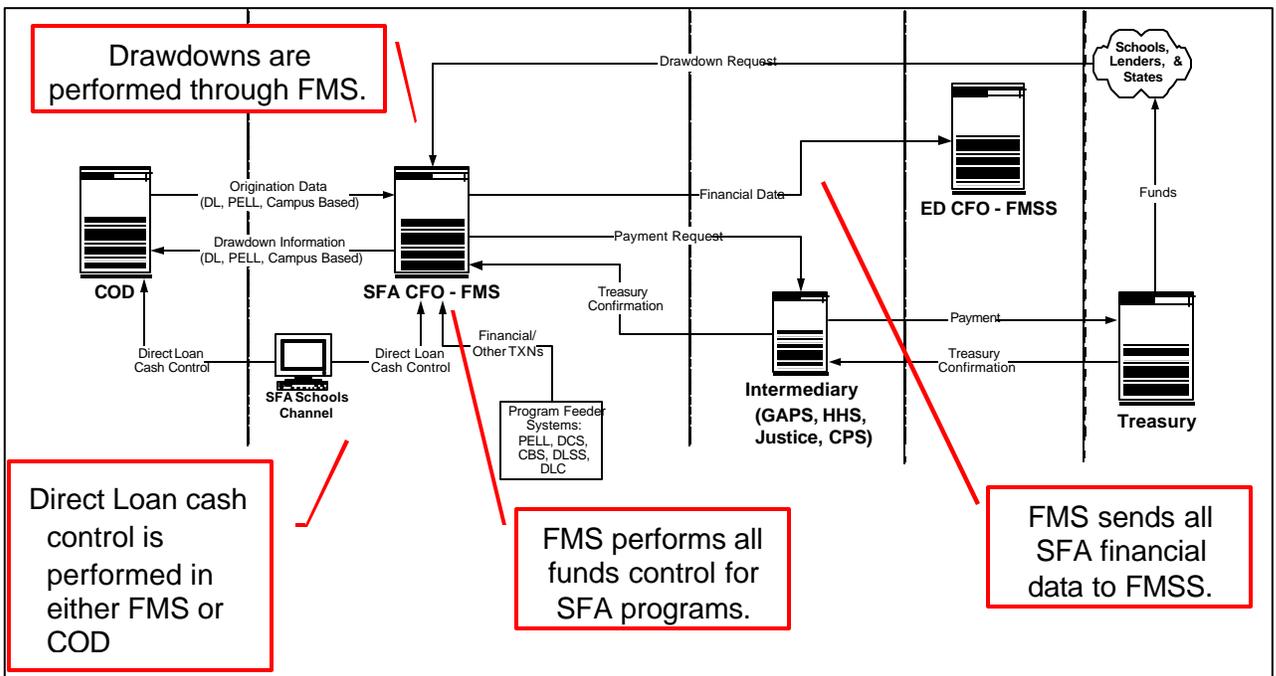
### FMS Phase III Interface Requirements (August 2001):



Future Releases – OCFO Interfacing Requirements:

Preliminary design for FMS Phase IV has identified the following items that will need to be coordinated between the SFA-FMS and OCFO-GAPS systems:

- SFA-FMS will provide all of SFA’s financial information to ED-FMSS.
- SFA Funds Control and Direct Loan Cash Control functionality will either be done in COD or move to the SFA-FMS system.
- SFA Drawdown and Refund Requests will be processed by the SFA-FMS system.
- SFA will use GAPS, or another system (e.g., Central Processing System [CPS]), solely as an intermediary for payment batches being sent to Treasury.



---

## **Guaranty Agency Migrations**

As previously stated, the Phase III architecture also supports Guaranty Agency on-line access functions currently performed under Phase II. The GA requirement to access their FMS functions via VPN can be eliminated by:

- Migrating current GA functions from the “internal” web/form servers to the “external” servers, and
- Integrating GAs into the Phase III HTTP file transfer process.

After migration, access via VPN can coexist with the Phase III architecture assuming the GA interface remains on the internal web/form server. GA training can be performed in phases; as GAs undergo training to use the new access method, their VPN and FTP userids can be deactivated.

The timing as to when the GAs will be converted to direct web access has not been determined.

---

## **Future Project Considerations**

There are several major initiatives either in progress at SFA or being considered that will likely impact the FMS technical architecture design at some point in the future. As the requirements for these initiatives are finalized, they will be analyzed to determine the impact to the FMS architecture. As a result, the FMS technical architecture may change. These initiatives include, but are not limited to:

- Enterprise Application Integration (EAI) – a set of common technology services that enable sharing of processes and data of disparate systems to support end-to-end business processes.
- E-Sign – electronic signature.
- Single Sign-On.
- SFA enterprise IT standards.
- Capacity Planning – as FMS' requirements and users grow, this may dictate changes to the existing architecture.

The timeframe for integrating with these initiatives has yet to be determined.