



**F E D E R A L
S T U D E N T A I D**

We Help Put America Through School

FSA Integration Partner

ED PIN Re-Engineering Analysis

ED PIN Technical Architecture Upgrade Analysis

Deliverable 131.1.3

Version 2.0

September 26, 2003

Amendment History

DATE	SECTION/ PAGE	DESCRIPTION	REQUESTED BY	MADE BY
Sept. 26	3.5	Addition of database considerations to capacity plan.	FSA	Integration Partner



Table of Contents

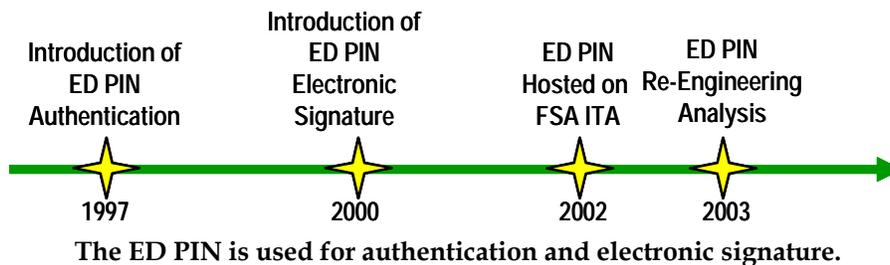
EXECUTIVE SUMMARY	4
1 INTRODUCTION	9
2 TECHNICAL ARCHITECTURE UPGRADE ANALYSIS	11
2.1 CONCEPTUAL DESIGN	11
2.1.1 Identification	11
2.1.2 Registration	13
2.1.3 Access	16
2.1.4 Self Service	18
2.1.5 Administration	21
2.2 REQUIREMENTS	23
3 CAPACITY PLANNING	33
3.1 NUMBER OF USERS	34
3.2 ED PIN PEAK USAGE PROJECTIONS	35
3.2.1 ED PIN Peak Usage Projection.....	35
3.2.2 Peak FAFSA Submission Projections	36
3.3 ED PIN USAGE TRENDS FOR 2003.....	37
3.3.1 Period of Maximum Activity	37
3.3.2 Usage Breakdown by Business Process.....	38
3.3.3 Cumulative ED PIN Hits for 2003 by Business Process.....	39
3.3.4 Monthly breakdown of Business Processes	39
3.3.5 ED PIN Peak Hour Usage by Month.....	40
3.4 ED PIN PEAK PERIOD PERFORMANCE PROJECTIONS	41
3.4.1 FAFSA and ED PIN Integrated Architecture	41
3.4.2 Performance Projections	42
3.5 ED PIN DATABASE CONSIDERATIONS	44
3.6 SUMMARY OF CAPACITY FINDINGS.....	46
4 CONCLUSIONS	47
APPENDIX A – REFERENCES	53
APPENDIX B – DEFINITION OF TERMS	55
APPENDIX C: ED PIN TRANSACTIONS PER HOUR AT PEAK (PROJECTED VOLUME) JANUARY 2002 - APRIL 2003	58



EXECUTIVE SUMMARY

The ED PIN Today

The ED PIN is a credential issued by FSA to students, parents, Title IV program financial aid administrators (FAAs) at higher education institutions and FSA trading partners. Except for FAAs, FSA verifies the SSN, name and DOB with the Social Security Administration prior to issuing the ED PIN. The credential is used in combination with personal data (SSN, 1st 2 characters of the last name and DOB) to authenticate users (i.e., gain access to FSA electronic services) and for certain electronic signature purposes associated with FSA transactions. The ED PIN is required for user access to FAFSA on the Web data or current status of processed data. It can also be used to access data stored within NSLDS¹ and perform certain transactions on the Direct Loan Servicing website and Direct Loan Consolidation website. Furthermore, FAAs use the ED PIN to perform business functions within FAA Access Online and E-Campus Based systems. Future uses of the ED PIN under consideration by FSA may include user authentication on the FSA Student Portal and inter-agency E-Gov projects. FSA's implementation of the ED PIN for user authentication and electronic signatures has been very successful with over 34 million ED PINs issued since 1997.



Purpose of the ED PIN Re-Engineering Analysis

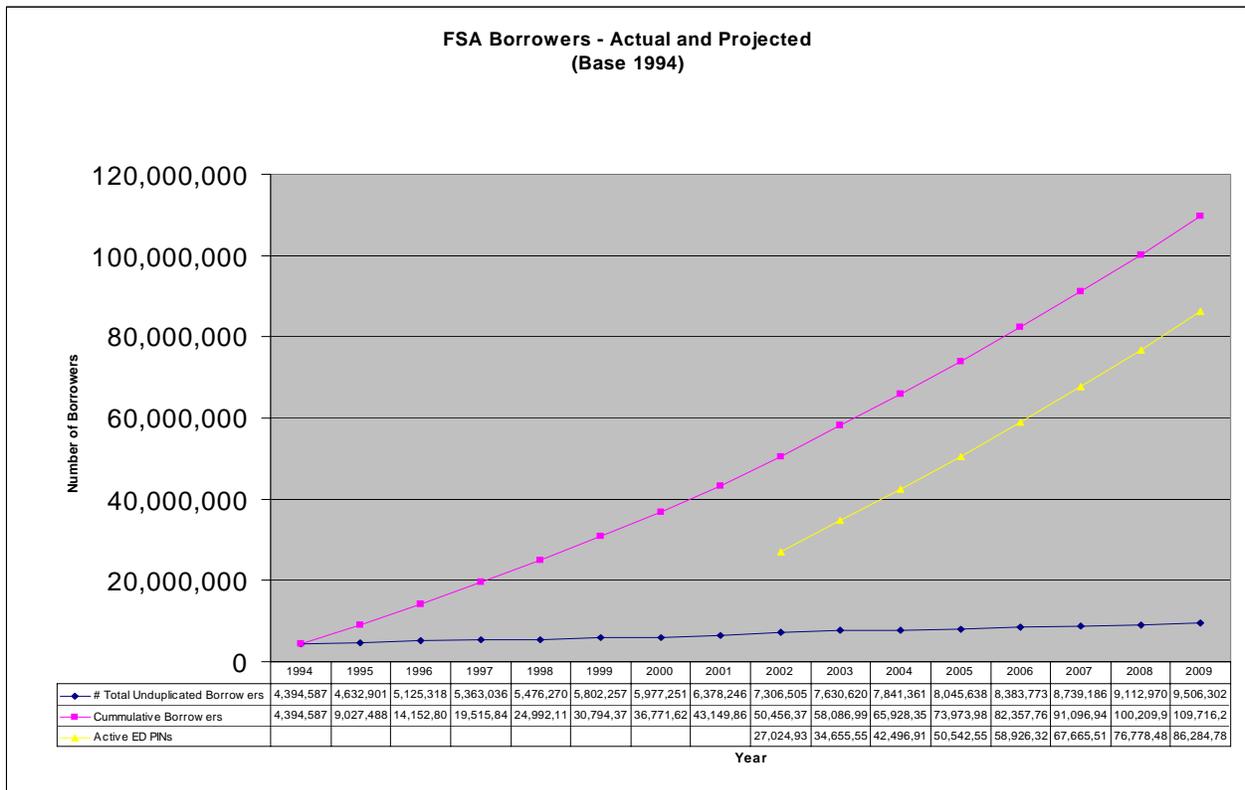
The ED PIN Re-Engineering Analysis is a high priority (#17, FY2003) FSA initiative to examine enterprise use of the ED PIN credential for authentication, its supporting processes and systems. The purpose of the analysis is to recommend an enterprise authentication solution that meets FSA's business requirements. The analysis concludes that the ED PIN is a suitable credential for authentication and electronic signature functions in support of borrowers (students and parents). The ED PIN does not lend itself as an authentication credential for trading partners. Conclusions also include specific recommendations to further strengthen the ED PIN integrity to enable it as the enterprise authentication service for all FSA borrower electronic services.

Recommendations

Recommendations from this analysis focus on re-engineering activities to (1) focus the ED PIN as a borrower credential only (student or parent), (2) enhance the integrity of the ED PIN credential, (3) develop additional administration and control functionality within the ED PIN system while standardizing its use across all the client systems, and (4) integrate the re-

¹ National Student Loan Data System.

engineered ED PIN credential with an FSA enterprise authentication solution. The specific recommendations noted in this document will provide FSA with the desired enterprise authentication service for all electronic services regardless of borrower life cycle stage. Allowing the credential to be used by a variety of customer groups other than students will continue to dilute the integrity of the credential for use in both authentication and electronic signature functions. The integrity issues with the current ED PIN data already present authentication and electronic signature problems. These problems will increase over time without proper controls. Strict controls around the use of the ED PIN and administration functions to support standard use of the functionality across the enterprise are also necessary to ensure ED PIN success. The longevity of the ED PIN will be severely limited without immediate attention to these requirements, especially in an environment where demand for electronic services is rapidly increasing.



Requirements

The analysis concludes that the ED PIN credential should provide a singular way to authenticate students, parents and borrowers. The practice of allowing multiple ED PIN records associated with an individual should be discontinued. It is critical to ensure that the integrity associated with the ED PIN credential is not compromised as increased number of customers use it for electronic services as well as increased number of applications rely on it for authentication. To ensure longevity of the ED PIN as the access management credential will also require strict enforcement of the business standards. To implement the recommendations, FSA will need to separate authentication and electronic signature functionality thereby enabling



the capability to ensure electronic access to all borrowers (including those without SSNs) without compromising electronic signature standards.

Business requirements, completed earlier during this project, demand that the ED PIN continue to be easy to use, comply with security, privacy, authentication and E-Sign standards, while supporting anticipated growth in FSA electronic services to customers. The potential number of FSA borrowers with the capability to access electronic services is expected to exceed 80 million by 2009. In support of Objective 5 of the Department of Education Strategic Plan – Enhance the Quality of and Access to Postsecondary and Adult Education², the ED PIN is a crucial asset to FSA services.

This stage of the ED PIN Re-Engineering Analysis focuses on a high level conceptual design for the re-engineered ED PIN process and associated requirements for an enterprise authentication solution. As requested, this stage of the analysis also provides capacity information for the current implementation of the ED PIN system.

The requirements analyzed in this document provide system, infrastructure and process information in support of an enterprise solution to meet the complete set of FSA’s business requirements. These requirements have been analyzed in coordination with the FSA Security and Privacy Technical Architecture Vision. Activities during this phase also focused on close coordination with FSA’s ongoing Data Strategy initiative particularly for the enterprise direction related to standard student identification method (SSIM), web services, enrollment and access management (EAM), technical strategies, web usage and integrated technical architecture. The requirements also incorporate Federal standards and policy guidance for e-authentication. A credential assessment analysis will need to be performed to ascertain the specific e-authentication level associated with ED PIN.

Conceptual Design

Recommendations for the re-engineered ED PIN solution include design and deployment of a set of standard and reusable components for identification, registration, access, self-service, and administration services. The re-engineered solution should possess identification components for both individual users and systems (ED PIN authentication clients) thereby possessing the capability to prevent unauthorized use of the ED PIN system by either users or systems. The

Individuals	IDENTIFICATION	Systems
Individuals	REGISTRATION	Systems
Authentication - Individual - System	ACCESS	Electronic Signature
SELF-SERVICE		
Alerts	ADMINISTRATION	Management Reports

ED PIN system should be used for the borrower community only (i.e., students and parents). The ED PIN is not a suitable credential for trading partners (schools and financial partners) including FAAs. A plan to transition FAAs to a different authentication credential should be developed as part of the Identity and Access Management (I&AM)

² U.S. Department of Education Strategic Plan 2002 – 2007.

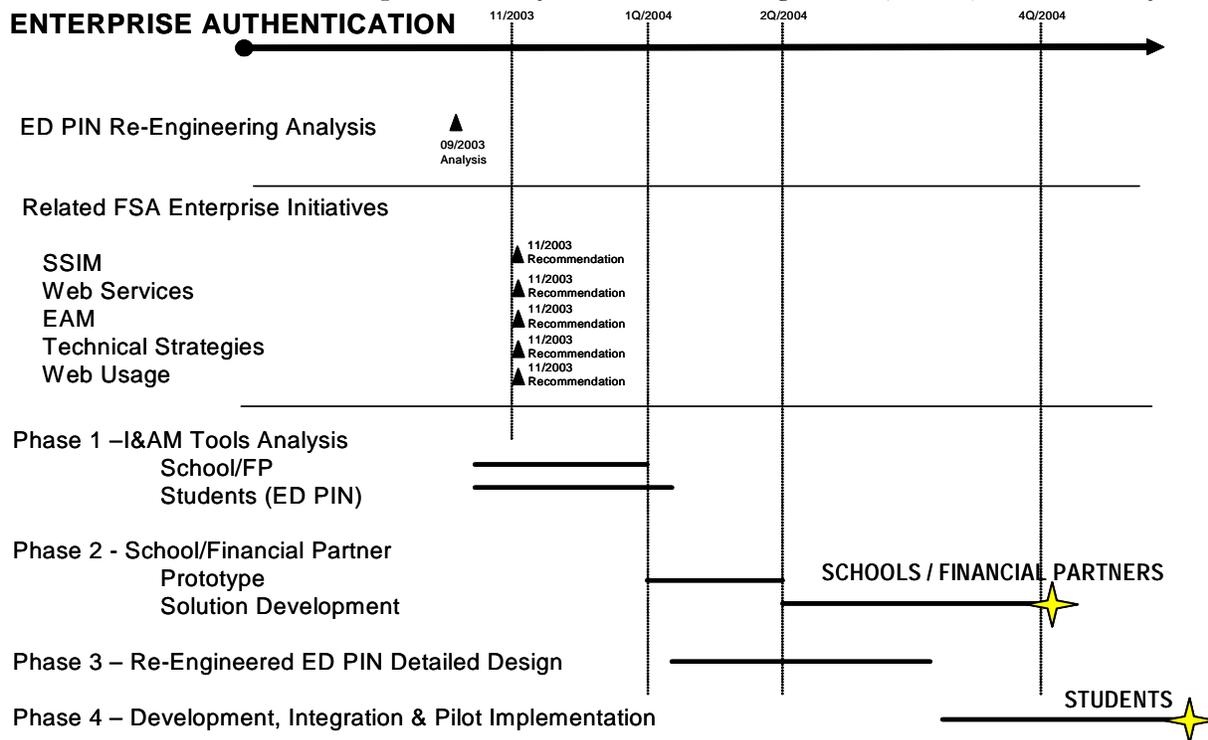


initiative. The registration process should continue to rely on SSA verification of individual information but also possess the flexibility for supplemental verifications with other government sources. Other government sources may include the Department of Homeland Security for terrorist alerts, the Department of Justice for prisoner lists, and other relevant sources as and when they are made available for use to the Department of Education. The registration process associated with client systems should also be formalized as an annual activity to ensure all requirements are known and tested. Functionality within the registration process should distinguish between individuals verified through the SSA match and other sources. The ability to distinguish between credentials that are verified with SSA and those that are not will allow FSA to service its entire student customer base (including individuals without social security numbers such as Pacific Islanders) without compromising compliance with electronic signature standards.

The access process should separate the distinct functionality associated with authentication and electronic signature. Authentication should be implemented for both individual users and client systems as part of any transaction request to the ED PIN system. Self-service functionality should be enhanced to encourage increased use of the ED PIN while minimizing help desk contact. And finally, the administration process should be strengthened as part of the re-engineering effort to include standard management reports as well as intelligent alerts associated with potential security and privacy threats.

Approach

FSA possesses a unique opportunity to develop the ED PIN enterprise authentication solution in coordination with the enterprise identity and access management (I&AM) effort already



underway. The I&AM effort focuses on a similar problem for trading partners (schools and financial partners). Coordinating activities with the I&AM effort will enable FSA to leverage synergies across the two distinct customer groups.

A 4-phased approach is recommended for establishing an FSA-wide enterprise authentication solution that includes both trading partners and students. The 3-phased approach incorporates decision milestones at the end of each phase to (1) ensure that goals for each phase are met and (2) provide an opportunity for FSA executive decisions in light of other enterprise priorities. The goal for Phase 1, Tools Analysis, are to participate in a joint tools analysis with the I&AM initiative and conduct a tools analysis to decide whether a commercial off the shelf (COTS) solution is cost beneficial or to continue development of an in-house solution. The tools analysis phase with the I&AM effort should attempt to ascertain whether a single enterprise solution can support both the trading partner (school and financial partner) and student business requirements. The goal for Phase 2, School/Financial Partner Prototype and Solution Development, is to implement a solution based on the results from the tools analysis for the schools and financial partner customers. The goals of Phase 3 are to (a) re-engineer and design the enterprise level processes for the 5 business functions associated with the ED PIN. This phase should leverage lessons learned from the prototype and incorporate best practices into the design. Phase 4, Development, Integration and Pilot Implementation, can then develop the student focused ED PIN authentication service as an extension to, or separate instance of, the I&AM TPM implementation.

The recommendations for a re-engineered ED PIN solution result in a comprehensive enterprise authentication solution for borrowers that can be leverage across all appropriate business processes. Such a solution will require focused communications with current users (both client systems and trading partners) to ensure transition activities are completed successfully.

Capacity Analysis

The capacity analysis performed during this phase utilized actual and projected Title IV program applicants to determine hardware infrastructure needs of the current ED PIN system. The ED PIN system does not have any critical infrastructure requirements beyond its current implementation on the FSA integrated technical architecture for the 2004 - 2005 school year. The capacity analysis provides infrastructure recommendations for both peak and off-peak transaction processing requirements. ED PIN transactions are expected to grow at an annual rate of approximately 25% for the next 6 years. Capacity projections will need to be re-examined upon completion of the re-engineered ED PIN system.

1 Introduction

The ED PIN process was instituted by the Department of Education Office of Federal Student Aid (FSA) in 1997. Originally designed to authenticate users utilizing the FAFSA on the Web product, the ED PIN is now leveraged across the FSA enterprise by other user-facing services that include system access and electronic signature functionality. The ED PIN processes are a CPS³ sub-system and are also used by internal FSA organizations (such as Schools) to support Title IV federal student aid processing. The ED PIN is used to authenticate users for web-based access to various FSA systems. The ED PIN system maintains authentication data for over 32 million users and is growing at an increasing rate as more customers begin to use FSA web-based products. FSA's ability to authenticate web customers for various services is critically dependent upon the integrity and availability of the ED PIN data. The ED PIN process also needs to support the potential for increased future use through standard processes and an infrastructure that is scaleable and robust.

The ED PIN is a credential issued by FSA to students, parents, financial aid administrators (FAAs) and FSA trading partners. Except for FAAs, FSA verifies the SSN, name and DOB with the Social Security Administration prior to issuing the ED PIN. The ED PIN is required for authenticating users' to access their FAFSA on the Web data or current status of processed data, access to their data stored within NSLDS⁴, access to Direct Loan Servicing website functions, access to Direct Loan Consolidation website functions, as well as for electronic signature capabilities⁵. FAAs at higher education institutions with Title IV student aid programs require an ED PIN to access the functions within FAA Access Online and E-Campus Based programs. Future uses of the ED PIN currently are under consideration by FSA and may include user authentication on the FSA Student Portal and e-gov initiatives.

The ED PIN Re-Engineering Analysis is a high priority (#17, FY2003) FSA initiative. The purpose of this initiative is to examine the ED PIN and its supporting processes from the perspective of future use. The ED PIN processes support Objective 5 of the Department of Education Strategic Plan - Enhance the Quality of and Access to Postsecondary and Adult Education⁶.

This analysis has led to the identification of ED PIN requirements for developing functionality in five distinct competencies. The requirements have been coordinated with activities underway on the FSA data strategy and security architecture initiatives. The five ED PIN competencies include:

- Identification
- Registration
- Access
- Self-Service, and

³ Central Processing System.

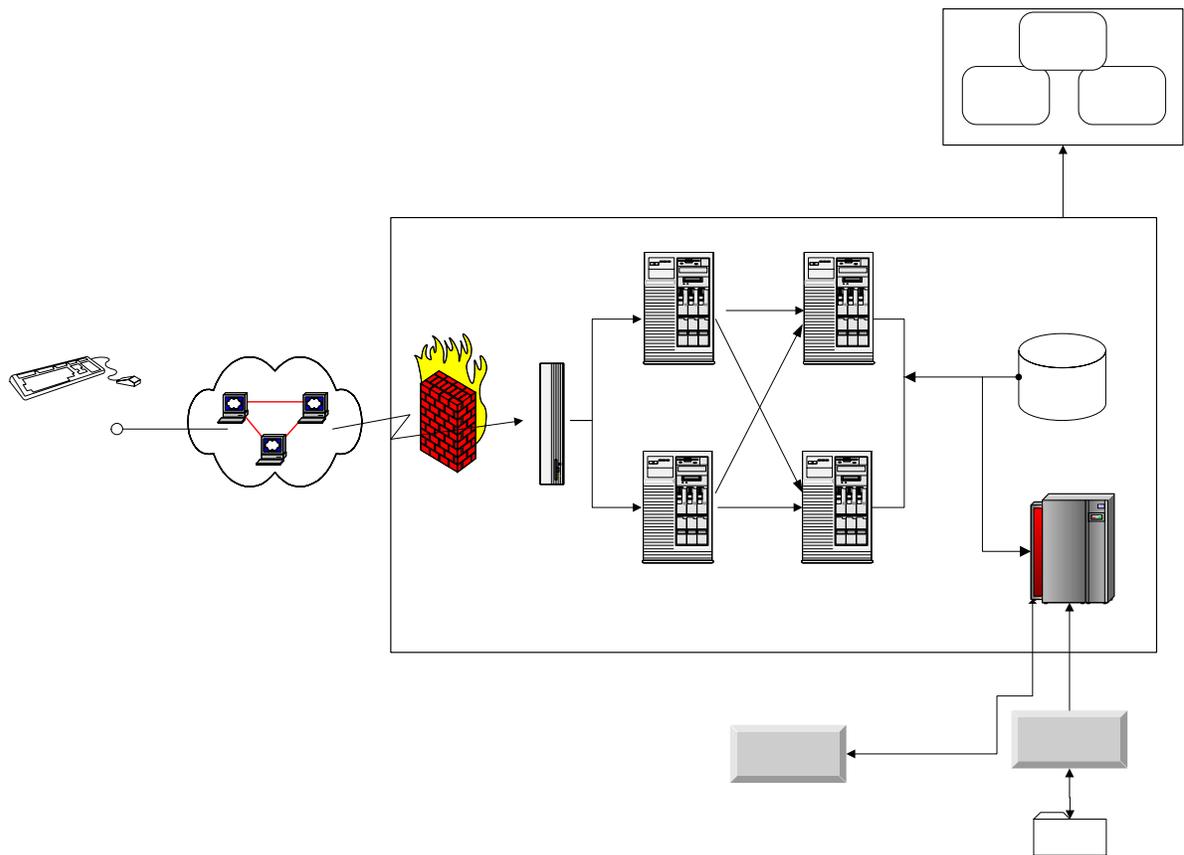
⁴ National Student Loan Data System.

⁵ For example, Promissory Notes.

⁶ U.S. Department of Education Strategic Plan 2002 - 2007.

- Administration.

Deliverable 131.1.2, completed earlier, analyzed all the current ED PIN processes, systems and associated interfaces. A high level logical overview is illustrated below. The current ED PIN system operates efficiently on the FSA integrated technical architecture and shares infrastructure with the FAFSA on the Web application system at the VDC. Some ED PIN system functions reside in CPS (e.g., edits and validation logic for data input interface from client system) or are outsourced (e.g., PIN mailers – e-mail and paper, customer support and electronic signature functionality).



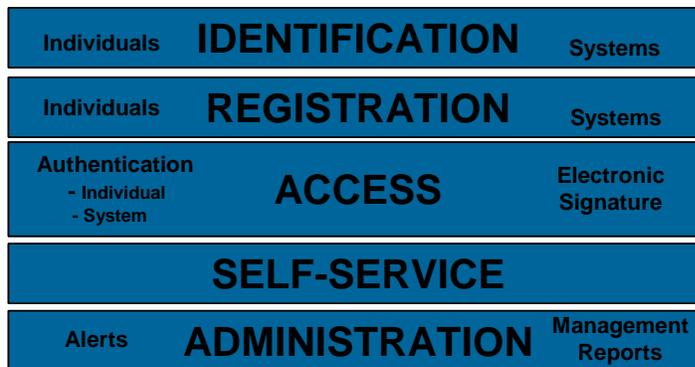
The analysis completed in Deliverable 131.1.2 identified findings to address shortcomings related to process and infrastructure, data administration and evolving standards. Working closely with client systems, the deliverable resulted in the compilation of business requirements and standards to address all the findings and enable the ED PIN as an enterprise authentication service for borrowers. This document elaborates on the business requirements and standards to establish the technical requirements for a re-engineered ED PIN process.

2 Technical Architecture Upgrade Analysis

The Technical Architecture Upgrade Analysis of the ED PIN System is based on the Business Requirements in deliverable 131.1.2 - Updated ED PIN Business Requirements and Standards. The following sections discuss a conceptual design with technical upgrade recommendations for a Re-Engineered ED PIN system. This system will be the Enterprise Authentication service provider for FSA. The capabilities of the Re-Engineered ED PIN system are categorized into five major services: Identification, Registration, Access, Self-Service, and Administration.

2.1 Conceptual Design

The following sections discuss the high level design created for the re-engineered ED PIN system. Recommendations for the re-engineered ED PIN solution include design and deployment of standard service solutions for identification, registration, access, self-service, and administration. The following model illustrates the five services.



2.1.1 Identification

The re-engineered solution should possess identification components for both individual users and systems (ED PIN authentication clients) thereby possessing the capability to prevent unauthorized use of the ED PIN system. The ED PIN system should be used for the borrower community only (i.e., students and parents). The ED PIN is not a suitable credential for trading partners including FAAs. A plan to transition FAAs to a different authentication credential should be developed as part of the Identity and Access Management (I&AM) initiative.

1.0 Identification

Individuals

- Social Security Number
- First Name
- MI
- Last Name
- Date of Birth
- Street Address
- City
- State
- Zip Code
- E-Mail Address
- Security Pass-Phrase
- Other items to possibly consider include gender, country, mailing vs. permanent address, driver's license, etc. Also open to consideration, required fields in addition to SSN, Last Name, DOB.

Systems

- Name
- Owner
- Technical Requirements
- 24 X 7 Contact(s)
- System Security Officer
- Production Date
- ED PIN functions used in addition to authentication (Functions may include authentication request, bulk processing of ED PIN registration, ED PIN update capabilities, deactivation request, etc.)
- ED PIN Authentication Mechanism (Standard API, Stored Procedure, Web Service, etc.)
- Number of transactions per function per day/week/month/year
- Maximum response time acceptable per function
- Utilization hours
- Transaction peak hours
- Transactions peak load during peak hours
- Average transaction load during utilization hours
- Batch window (if applicable)
- Test Information
- Maximum Transactions

2.1.2 Registration

The registration process should continue to rely on SSA verification of individual information but also possess the flexibility for supplemental verifications such as those with terrorist, prisoner and other sources. The registration process associated with client systems should also be formalized as an annual activity to ensure all requirements are known and tested. Functionality within the registration process should distinguish between individuals verified through the SSA match and other sources. This functionality will allow FSA the capability to service its entire student customer base including individuals without social security numbers (e.g., Pacific Islanders). The numeric notification in the following paragraphs are references to illustrated processes.

Registration (Client Systems) - All potential Client Systems (FSA systems (2.1.1) and non-FSA systems (2.1.2)) must undergo a formal process to use the ED PIN on an annual basis. The process will involve the requesting system owners to provide specific information about their system and needs (2.1.3). After acceptance by the ED PIN system owner, technical specifications and protocol for interfacing with the ED PIN system are issued to the client system (2.1.5). After successful testing of the interface (2.1.6), the ED PIN registers the System and authorizes interface with the ED PIN system.

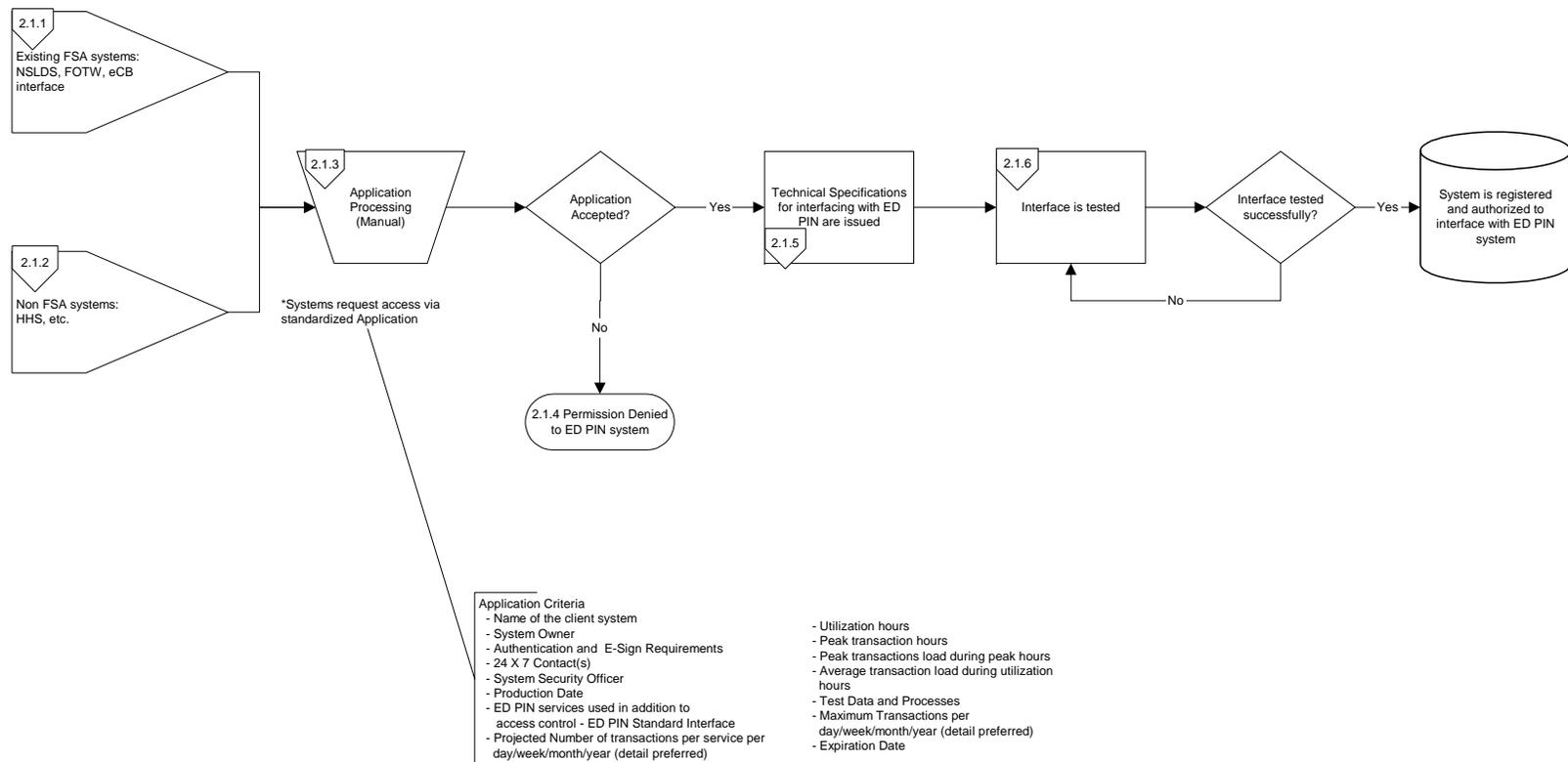
Registration (Individuals) - An ED PIN application may be initiated from the ED PIN site, another registered FSA system, and from system to system generation from registered FSA systems (2.2.1, 2.2.2, 2.2.3, 2.2.4, 2.2.5). For individual processes the user will enter their required data (2.2.6). Upon a syntax check of the data, the ED PIN system will then perform the SSA match(2.2.7, 2.2.8) for records with standard nine digit SSN's. Matched records will have ED PIN records created on the ED PIN Database and users will be notified of their ED PIN (2.2.13). Non-standard (pseudo) SSN's will originate from other FSA systems only for an ED PIN on behalf of their customers. Since, these records did not undergo an SSA verification, these records will not be e-sign enabled. In addition, supplemental 3rd Party verification with other agencies may be required prior to record creation in the ED PIN Database (2.2.10). Should an application request not be formatted correctly, fail the SSA match, or the 3rd Party Verification process, the ED PIN record will not be created (2.2.11) and the result will be added to an error log (2.2.12).

ED PIN Re-engineering Process Design

Process: Registration (Client Systems)

Process ID: 2.1

Description: The standardized process of authorizing and registering systems for interface with ED PIN System

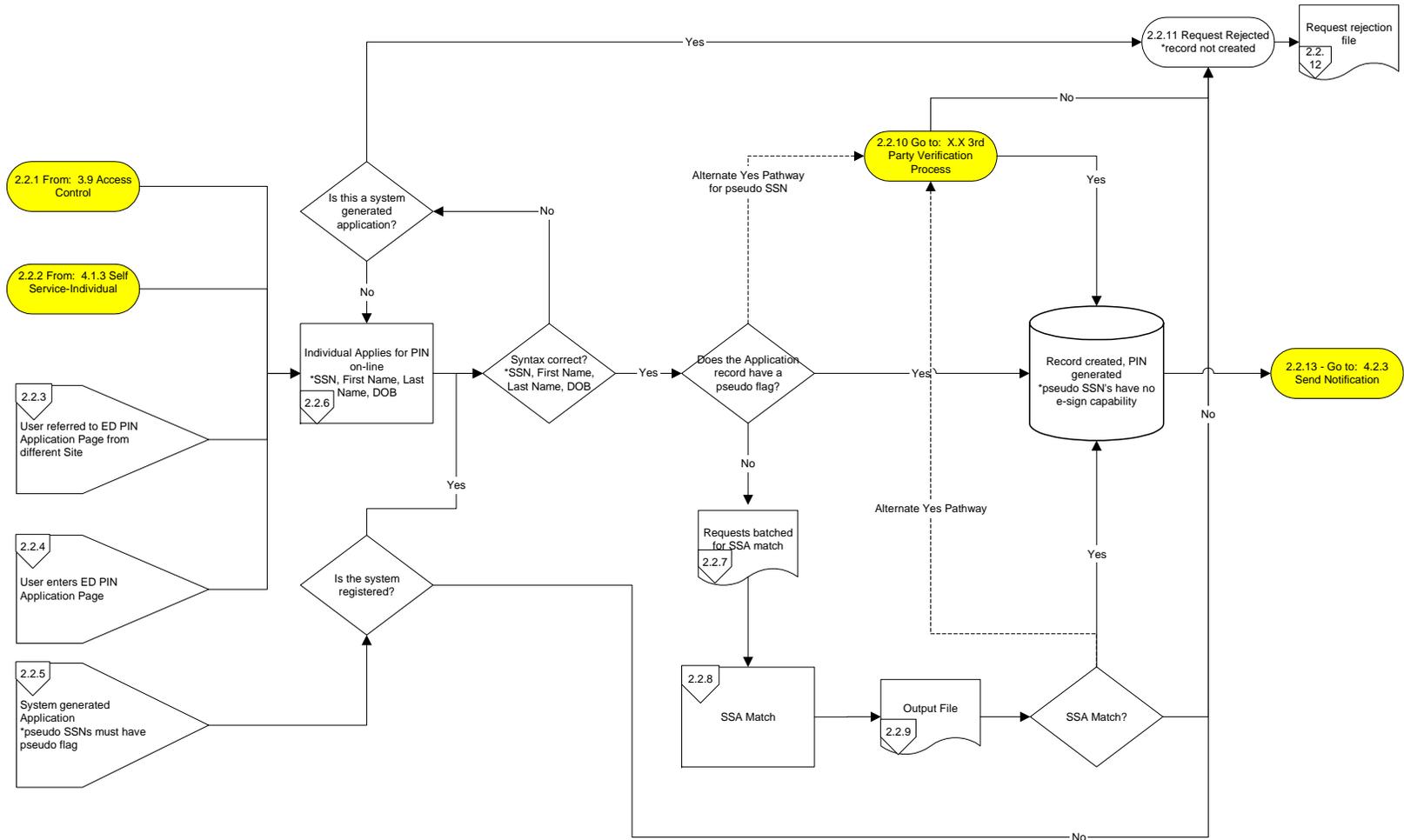


ED PIN Re-engineering Process Design

Process: Registration (Individual)

Process ID: 2.2

Description: The process of applying for ED PIN



2.1.3 Access

The access process should separate the distinct functionality associated with authentication and electronic signature. Authentication should be implemented for both individual users and client systems as part of any transaction request to the ED PIN system.

Access Control – Can be initiated by FSA client systems or for certain functions on the ED PIN site. Client systems communicating with the ED PIN system (3.1) must be verified by the ED PIN system. If the system is not registered or verified, the request is rejected and logged (3.4, 3.5).

If the system is verified or if the authentication is from the ED PIN site (3.2); then the request enters the Authentication process (3.3). The request can be a request for authentication or an e-Signature.

Users are authenticated on the basis of a data match relative to within the ED PIN system for a user (3.10, 3.12). If the authentication request is unsuccessful, the ED PIN system will determine if there is a record for this user. If not, the user is pointed to the application process (3.9). If the user record exists, the record undergoes a series of checks. If this is the user's 50th unsuccessful attempt, an alert is generated and the user is notified (3.7, 3.8). If this is the 3rd consecutive unsuccessful attempt or the 6th unsuccessful attempt in a 24 hour period, then the record is locked for the remainder of the day (3.6) and the user is notified (3.8). If the user has forgotten their ED PIN, they may request their PIN be sent to them (3.15, 3.8). If the user does not request their ED PIN, then they are sent back to the place of origin to attempt authentication again.

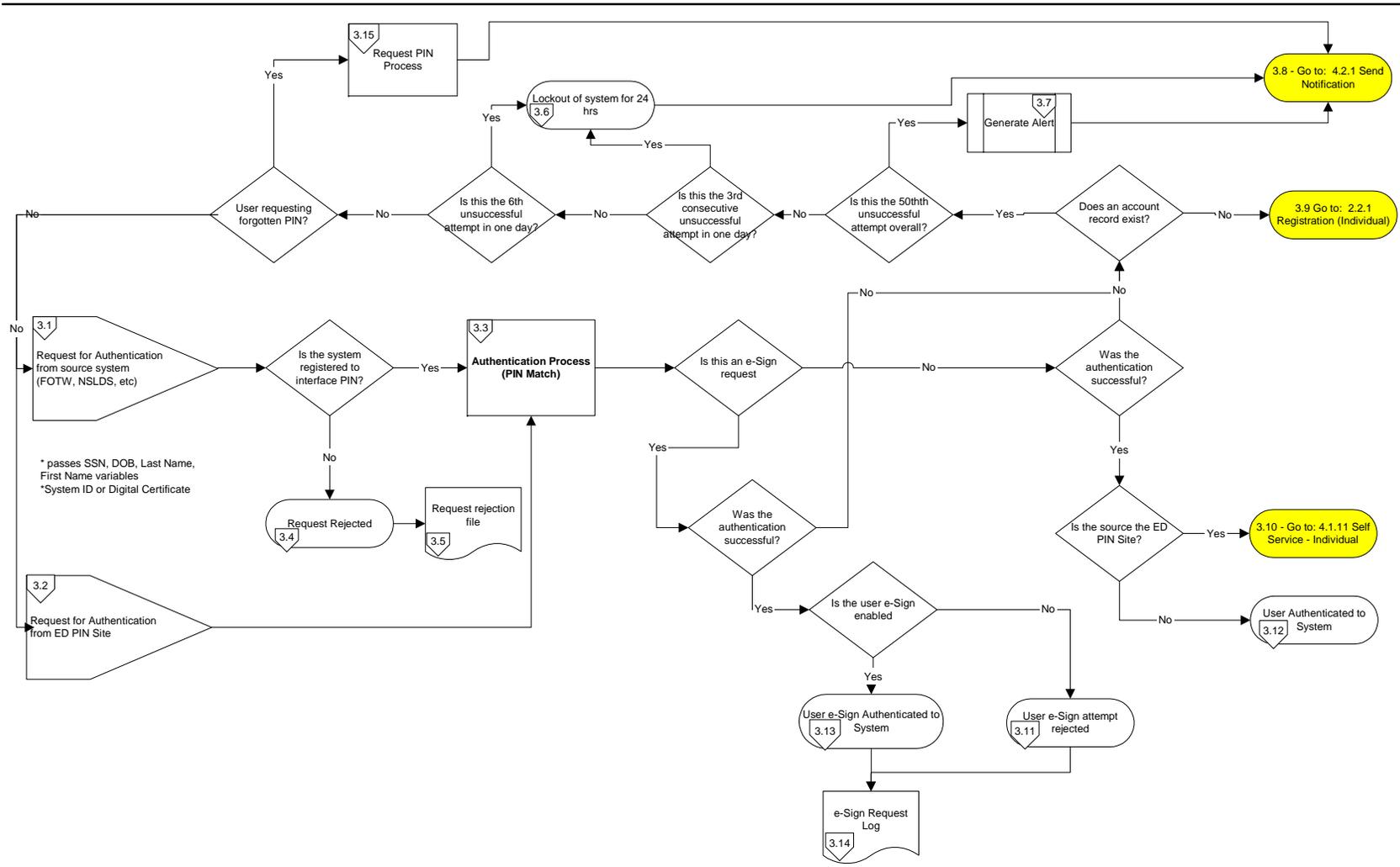
If the request is for an e-signature, the user is authenticated and the system determines whether the ED PIN is e-sign enabled. If the user is e-sign enabled, the ED PIN system authorizes (3.13) and logs the e-sign request (3.14). If the ED PIN is not authenticated or is not e-sign enabled, the e-signature is not authorized (3.11) and is recorded (3.14) in the error log.

ED PIN Re-engineering Process Design

Process: Access Control

Process ID: 3.0

Description: The process of authenticating a client system or user (student, parent, borrower, etc.)



2.1.4 Self Service

Self-service functionality should be enhanced to encourage increased use of the ED PIN while minimizing help desk contact.

Self-Service (General) – This process flow describes the various capabilities ED PIN users will have in maintaining their account. Upon entering the ED PIN site, the user will have the option of checking the status of the account. If the user record does not exist, they are referred to the ED PIN application process (4.1.3). If the application is pending, the Application Pending status is displayed to the user (4.1.4). If the application is not pending, the record undergoes a series of status checks related to the state of the account. If the account is active, the user can either request their ED PIN (4.1.23, 4.1.20) or authenticate to the ED PIN site and perform various self service functions (4.1.2). If the account is not active, a series of additional checks on the record are performed. If the account has been user disabled, the status is displayed (4.1.5) and the user has the option of re-enabling the account via a user created pass phrase (4.1.9, 4.1.10). If the account is in a lock out state, the Account lock out status is displayed (4.1.6). If the account is de-activated, the Account De-activated status is displayed (4.1.7).

Other self-service capabilities will require authentication (4.1.2). Upon successful authentication (4.1.11), users will be able to disable their account (4.1.13, 4.1.14) via selection of a pass phrase (4.1.12). Users will also be able to update demographic information such as First Name, Last Name, Address, Phone Number, Pass Phrase, and their PIN (4.1.17). Changes to SSN are not allowed and changes to Date of Birth (4.1.15) will be subject to manual exception processing and are subject to SSA verification (4.1.16). Users may also update their e-mail address (4.1.18) upon confirmation of a valid e-mail address (4.1.19).

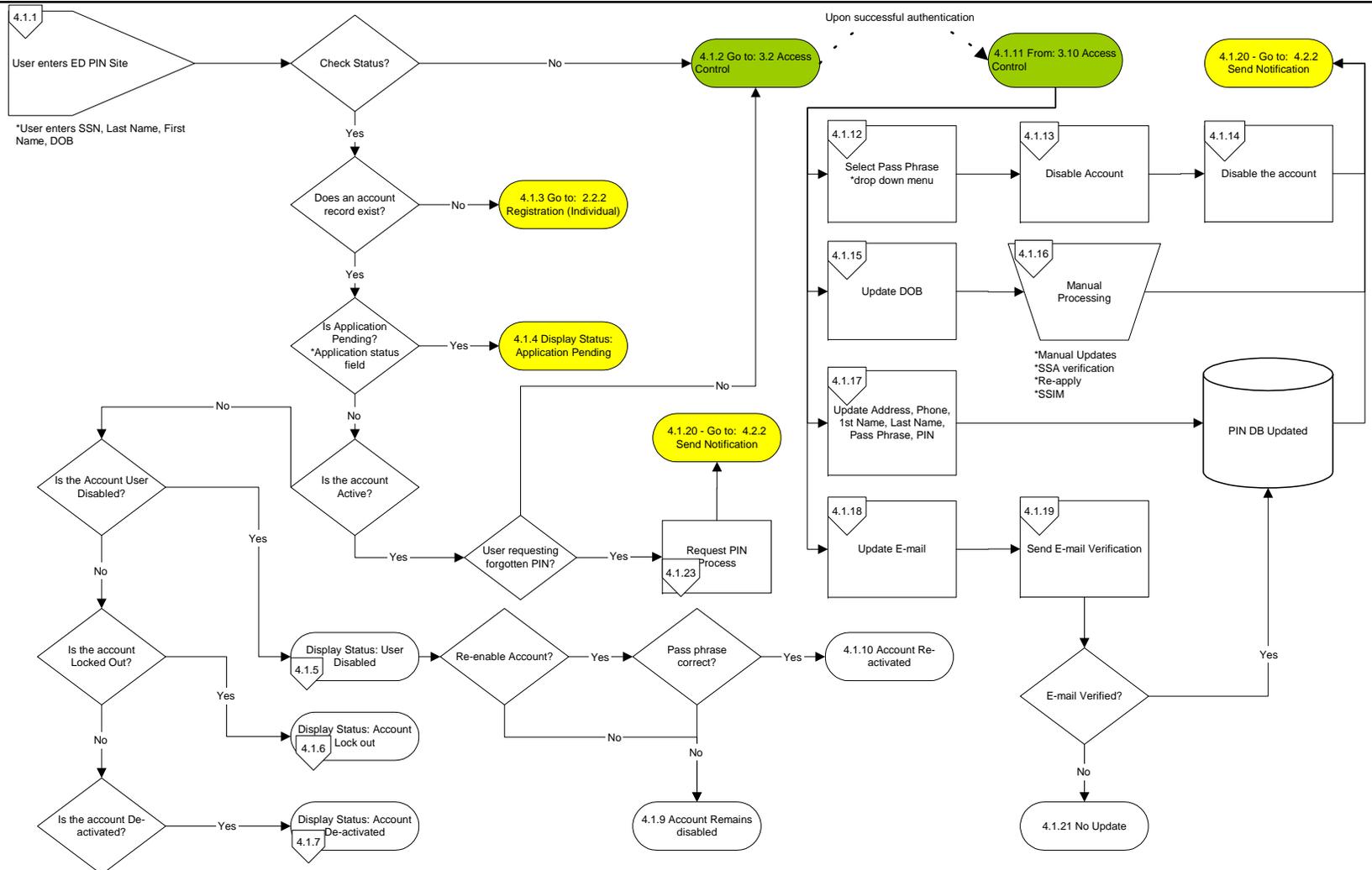
Self-Service (Notification Process) – Any Notifications, Alerts, and Information generated by the ED PIN system (6.1, 6.2, 6.3, 6.8) will be communicated via e-mail whenever possible (6.4) and logged (6.7). In situations where e-mail address is not available, paper notification will be sent in the instance of PIN issuance or PIN requests (6.5).

ED PIN Re-engineering Process Design

Process: Self Service - Individual

Process ID: 4.1

Description: Describes flow of all functions users can perform on their account

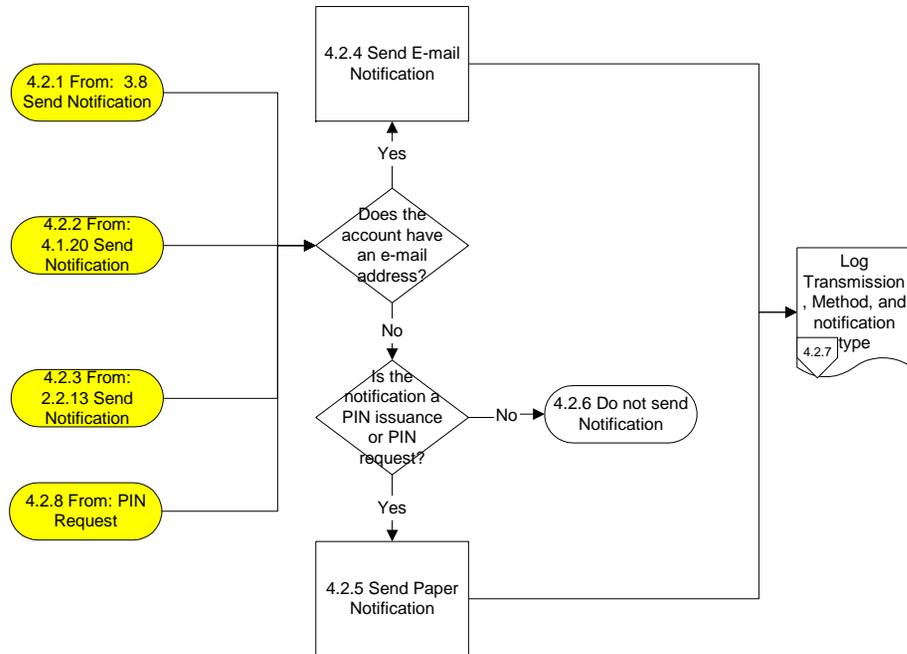


ED PIN Re-engineering Process Design

Process: Self Service (Notification Process)

Process ID: 4.2

Description: The process of Sending Notification to Users



2.1.5 Administration

The administration process should be strengthened as part of the re-engineering effort to include standard management reports as well as intelligent alerts associated with potential security and privacy threats.

Reporting Capability

The ED PIN system will include reporting functionality. Reporting elements may include the following:

- Total Hits
- Hits per Visit
- Average Visits per Day
- Average Length per Visit
- Pages Viewed
- Number of times Pages Viewed
- User Errors Encountered including Number of Errors
- Browsers used to visit ED PIN
- Failed Authentications
- Failed Electronic Signature transactions
- Client System Usage by function
- Client System pseudo-SSN transactions
- Self Service Reports for most used Functions
- Number of Records disabled, enabled, ED PIN changed, demographic updates
- Average Response Time
- Peak Transaction Hours
- Peak Transaction Load during Peak Hours
- Number of Batch Jobs
- Number of ED PIN mailers
- Number of ED PIN e-mails
- Total and Concurrent Users
- Total and Concurrent Client Systems
- Overall Availability
- Average time till e-mail notification

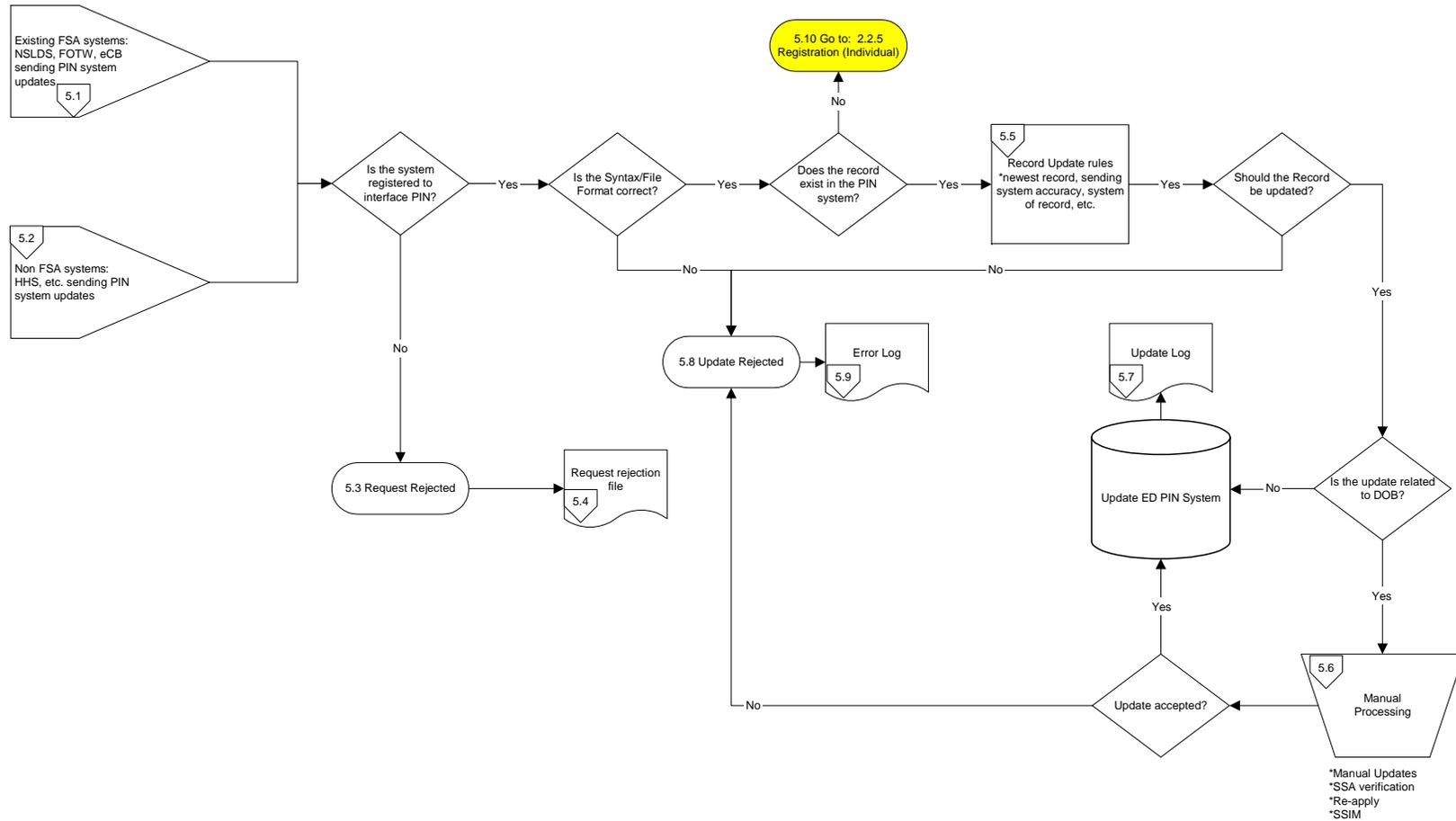
FSA/External Source System Updates – Source System Updates can come from FSA or Non-FSA systems (5.1, 5.2). Both types of systems must be registered to the PIN system in order for the PIN to receive updates. Should the system fail to authenticate itself, the update request is rejected (5.3) and logged (5.4). If the system is registered, then the file sent will be checked to confirm it is in the proper format, whether the record to be updated exists in the PIN Database. Any records not meeting the criteria will not be updated in the PIN Database (5.8) and will be logged (5.9). Records that meet the criteria will be subject to Update rules based on the source system and the most recent information (5.5). Records not meeting update rules will not be updated in the PIN Database (5.8) and will be logged (5.9). Updates regarding Date of Birth will be subject to manual exception processing and are subject to SSA verification (5.6). Records meeting all the above criteria will be updated in the PIN Database.

ED PIN Re-engineering Process Design

Process: Administration - FSA and External Client System Updates

Process ID: 5.0

Description: Client system agreement for using ED PIN



2.2 Requirements

The requirements noted in this section are based on the business requirements and standards completed earlier during the analysis and the conceptual design for the re-engineered ED PIN processes.

NO.	REQUIREMENT
1	The ED PIN system is an authentication facility and not an identity management system of record.
1.1	Web-based borrower authentication will be performed using the ED PIN system.
1.2	All business logic for ED PIN system functionality will be part of the ED PIN system.
1.3	The ED PIN credential will be the enterprise access method for all FSA borrower electronic services.
2	FSA client systems authorized to use the ED PIN for authentication and subsequent granting of any type of access or information on the basis of the ED PIN will document their technical implementation.
2.1	All potential client systems will adhere to the annual registration/update and interface process. This process is yet to be developed.
2.2	<p>At a minimum, client systems must provide or update to the degree they are known, the following data elements during the annual process.</p> <ul style="list-style-type: none"> - Name of Client System - System Owner - Authentication and e-Signature Requirements - 24 X 7 Contact(s) - System Security Officer - Production Date - ED PIN service required - ED PIN standard interface - Number of transactions per service per day/week/month/year - Utilization hours - Peak transaction hours - Peak transactions load during peak hours - Average transaction load during utilization hours - Test data, plan and processes - Maximum Transactions per day/week/month/year
2.3	Interface must be integration and system tested before client system is authorized to authenticate with ED PIN.
2.4	ED PIN system owner must approve use of ED PIN credential for client system.
2.5	ED PIN system must be executable on FSA ITA.
2.6	ED PIN system must comply with FSA SLC.
3	The ED PIN system will incorporate the Generally Accepted System Security Principles

NO.	REQUIREMENT
	(GASSP) as adopted by the Department. These principles will include pervasive principles that address Confidentiality, Integrity and Availability. Additionally, the ED PIN system will support protection against discovery and misuse of identity by other users.
3.1	The ED PIN system will support anonymity – i.e., user can use a resource without disclosing the user’s identity to other users.
3.2	The ED PIN system will support Pseudonymity – i.e., user’s identity is not disclosed to other users but the user is still accountable for its action.
3.3	The ED PIN system will support Unlinkability – i.e., user can use a resource multiple times without other users being able to link these sessions to each other.
3.4	The ED PIN system will support Unobservability – i.e., user can utilize a resource without unauthorized parties being able to observe his/her actions or usage.
4	The ED PIN system will conform to the FSA Security Architecture.
4.1	The ED PIN system will possess access management, provisioning, directory service functions.
4.2	The ED PIN system will have the capability to support multiple directories for access at the same time.
4.3	The ED PIN system design will be scalable to support FSA’s enterprise authentication needs and number of projected users (over 50 million active users by 2009).
4.5	The ED PIN system will scale to meet the capacity needs of client systems.
4.4	The system shall support SAML assertions to authenticate users.
5	The ED PIN access credential enforces user and administrator accountability and is used to prevent unauthorized people or processes from entering a client system.
5.1	Identity will be established using SSN, DOB, first name and ED PIN.
5.2	The ED PIN credential will support authentication.
5.3	The ED PIN credential will support electronic signature.
5.4	Electronic signature functionality will not be permitted without a positive SSA match.
5.5	The ED PIN credential cannot be stored within any client system.
6	The ED PIN access credential is used by users for access to user data maintained in client systems.
6.1	The ED PIN credential cannot be used to access privacy data or records for other individuals.
7	The ED PIN credential is not required for general access to FSA resources where no transactions are conducted and there is no privacy, confidential or other personal or sensitive data.
7.1	Anonymous access will be available at a minimum to the ED PIN system homepage, registration page and self service page.
8	Any access to the ED PIN user data by other than the user is not permitted, including for system tests.
8.1	Business logic to update customer record associated with the ED PIN credential will be maintained within the ED PIN system.

NO.	REQUIREMENT
9	It is the responsibility of authorized client systems utilizing the ED PIN for user authentication to test the functionality in coordination with the ED PIN system owner.
10	The ED PIN is required by users interfacing with FSA via the Internet to identify them uniquely before being allowed to perform any transactions on client systems.
11	The ED PIN will not provide authorization functionality for any FSA client system. Any authorizations (access control, access rules or role-based access) are the responsibility of the client system. Client systems may grant varying levels of authorization to users on the basis of ED PIN authentication.
11.1	The ED PIN system will be used for authentication and electronic signature purposes only.
12	The ED PIN will provide an enterprise shared service for authentication that can be used by FSA client systems. The ED PIN will not link actions to specific users except for ED PIN functionality - identification, registration, access, self-service, and administration.
12.1	The ED PIN system will publish performance standards associated with access functionality.
12.2	The ED PIN system will support standard and ad-hoc administrative and management reports.
13	The ED PIN will support the FSA Electronic Signature standards consistently.
14	The ED PIN architecture will integrate with the FSA Integrated Technical Architecture and include the appropriate redundancy, backup and recovery, disaster recovery, etc.
14.1	The ED PIN architecture will support redundancy with built-in fail-over capabilities.
14.2	The ED PIN system will be available 24x7x365 except as authorized by the Department.
14.3	The ED PIN system will include monitoring functionality to ensure availability and provide alerts in case of system malfunction.
14.4	The ED PIN system will comply with the FSA disaster recovery and continuity of operations policy.
15	The ED PIN will conform to Federal authentication standards. Any exceptions to Federal, Department of Education, or FSA policy will be documented.
15.1	A credential assessment will be performed for the ED PIN to determine its specific level as proposed in the Federal e-authentication guidelines.
16	The ED PIN credential data is established through a 3rd party verification match with the U.S. Social Security Administration (SSA). The ED PIN system will share the SSA 3rd party verification match functionality as a service; currently available in CPS.
17	The ED PIN credential does not expire.
17.1	The ED PIN system will maintain auditable logs associated with any activation/deactivation.
18	Any ED PIN record deletions from the repository will be auditable.
18.1	All transactions and changes associated with the ED PIN will be maintained in an auditable history log.
18.2	Deactive ED PIN records will be archived per FSA archive policies.

NO.	REQUIREMENT
19	ED PIN application is only available via the ED PIN site (www.pin.ed.gov) and not available via paper application or any other option except as authorized by the Department.
20	For user authentication, the ED PIN requires use of the user's social security number, first 2 characters of the last name, date of birth and the ED PIN.
20.1	Duplicate ED PINs associated with a user will not be permitted.
21	Any action requiring user authentication on the ED PIN system will require the use of the ED PIN access credential for that user.
22	All ED PIN authentication data is protected with access controls and encryption to prevent unauthorized individuals, including system administrators and customer support representatives, from obtaining the data.
22.1	Encryption standards will comply with NIST guidelines.
23	Any ED PIN access credential transmission (including between the components of the ED PIN system as well as user directories) requires that it be transmitted securely.
24	The ED PIN will be protected as it is entered into any system including suppressing the display of the ED PIN as it is entered.
25	A configurable number of unsuccessful attempts in using the ED PIN access credentials will automatically deactivate the ED PIN for a specified duration.
25.1	Daily unsuccessful authentication attempts will initially be 6 attempts per day or 3 consecutive attempts per day.
25.2	Deactivation periods will be configurable; initially to end of day (midnight).
26	The ED PIN data will be administered by authorized personnel.
26.1	The ED PIN data administration will include interfaces to other authorized client systems utilizing the ED PIN.
26.2	Administration personnel for the ED PIN system will be approved by the ED PIN system owner and comply with Department system administration guidelines.
27	The ED PIN permits the use of 4 numeric or 6 alphabetic characters as the ED PIN. Sequential numbers are not permitted. 6 alphabetic characters are supported but not used for the issuance of new ED PINs.
27.1	New ED PIN credentials issued will use 4 numeric characters.
28	Under normal circumstances, the ED PIN is not required to be changed periodically. The ED PIN may be changed by the user, may be disabled by the user and subsequently enabled by the user, and may be deactivated (including interruption of on-going user session) by the Department of Education under certain circumstances.
28.1	The ED PIN system will have self service functions.
28.2	ED PIN system self service functions will include the ability to disable and enable the ED PIN, change the ED PIN, request an ED PIN, retrieve a forgotten ED PIN, update permissible user data fields.
28.3	The ED PIN self service functions will support the use of advanced authentication (drop-down pass-phrase categories).
29	A temporary (or Guest) ED PIN is not issued.



NO.	REQUIREMENT
30	All users are notified not to use an easy-to-guess ED PIN, not to divulge their ED PIN, and not to store their ED PIN where others can find them.
30.1	The ED PIN system will enforce complexity rules to deter easy to guess ED PIN credentials.
30.2	The system will not allow the creation of a null ED PIN.
31	Advanced authentication (a challenge-response system) will be used to disable their ED PIN and re-enable their ED PIN.
32	Advanced authentication (such as cryptographic keys or tokens) will be used for authorized system administration associated with any ED PIN function.
33	Physical access to the ED PIN system components will be controlled.
33.1	The ED PIN system is accessible through a supported browser.
33.2	Client system access to the ED PIN system will require verification.
34	The ED PIN cannot be communicated, securely or otherwise, in any way to any one (including administrators) other than the user. Communication of the ED PIN to the user is only permitted in a secure transmission.
35	Users using the ED PIN will be informed why this type of authentication is used.
36	Users will also be told what authorized client system access is permitted with the ED PIN.
37	The ED PIN credential is unique to support individual accountability and authentication. An ED PIN can not be issued to a group or organization. An ED PIN can not be issued anonymously.
37.1	The ED PIN system will utilize a configurable identifier; current implementation will be SSN.
37.2	Issuance of an ED PIN credential for pseudo-SSN records in other FSA client systems will be permitted.
37.3	The function of issuing an ED PIN credential associated with a pseudo-SSN will be available as a service to client systems only.
37.4	An ED PIN credential associated with a pseudo-SSN will not be enabled for electronic signature functionality.
38	There are no roles associated with a user and their associated ED PIN. Any role-based authorization based on authentication with the ED PIN system is the responsibility of the business process using the ED PIN as an authentication service.
39	The ED PIN system is available 24 X 7 X 365, within FSA service level agreements, except as authorized by the Department.
40	There are no service constraints for users to use the ED PIN system (i.e., no restriction on how many times the system is used).
41	The ED PIN system will not provide search capabilities to users.
42	All access to the ED PIN system will be monitored.
42.1	Audit logs of all access requests will be maintained.
42.2	Audit logs of all security events with client system identity (including IP addresses) containing origin, results, date & time stamps will be created.

NO.	REQUIREMENT
43	Access to specific ED PIN functions for which users do not have access is never allowed.
44	The ED PIN system physical infrastructure will be protected in compliance with Federal regulations. These protections include port protection, secure firewalls and gateways, intrusion detection, real-time monitoring, etc.
45	The ED PIN system will possess the capability to send reminder notifications.
45.1	The ED PIN messaging service for notification will support all customers.
45.2	The ED PIN messaging service will comply with Federal, Department and FSA IT and security policy requirements.
45.3	The ED PIN system messaging service will include functionality for mass mailings.
45.4	The ED PIN system messaging service will include options for handling message delivery.
45.5	The ED PIN system messaging service will include monitoring functionality.
46	Keystroke monitoring will not be utilized in any activity associated with the user's use of the ED PIN.
47	Any ED PIN authentication data stored on client desktops must be encrypted. Permanent cookies with ED PIN authentication data are not permitted.
47.1	Only volatile (non-persistent) cookies will be used, if necessary.
48	The ED PIN system will not permit the retrieval of more than one ED PIN during a single transaction.
49	Session management standards will comply with the Department policy. These standards will include new session established with a client every time an HTTP request reaches the ED PIN server, a session will be terminated at a pre-determined time interval after the last activity, etc.
49.1	The session identifier must be generated randomly by a generator guaranteeing high statistical variance.
49.2	The ED PIN session state will be pre-determined by application code.
49.3	Leaving the Secure Socket Layer will terminate the session (e.g., navigation out of SSL).
49.4	A session that has remained idle (no requests) for a configurable duration must be automatically terminated.
49.5	Session identifiers will be encrypted and protected from interception.
50	Only server-side data input validation is permitted.
51	All users must be notified that the ED PIN system is a U.S. Government service and malicious activity may be monitored.
52	The ED PIN system will not provide single sign-on functionality. Use of the ED PIN access credential by any single sign-on process (including password synchronization, etc.) either internal or external to FSA will require prior approval from the ED PIN system owner. The ED PIN system will comply with the FSA Access and Enrollment Management Policy (in development).
53	There are no restrictions for the number of times users may change their ED PIN on an active ED PIN access credential.
54	The ED PIN system will allow batch registration (bulk processing) for user ED PINs

NO.	REQUIREMENT
	from FSA client systems authorized to perform this functionality.
54.1	Batch registration functions used by client systems will be approved during the client system registration process.
55	Users will be notified by the registered FSA client system submitting a registration request that an ED PIN will be requested on their behalf. There is variable text on the ED PIN e-mail notification and the ED PIN paper mailer that informs the recipient why the ED PIN was generated. While there is no advance notice given to a user in all instances, users will be provided an explanation upon receipt of the ED PIN.
55.1	New ED PIN credentials issued as a result of processing paper FAFSA's will be communicated via e-mail, if available.
56	The ED PIN functionality is for individual use only. Any delegation associated with an individual ED PIN is not permitted.
57	The ED PIN system design supports multi-vendor components.
58	Use of the ED PIN in other registered client systems is restricted to access functions only.
59	In the event of an ED PIN system outage an alert message will be posted on the ED PIN web site.
59.1	An alert message will be communicated to appropriate client system owners as identified during the registration process.
59.2	Security alert message generation capability will be customizable.
60	The end-user facing ED PIN authentication screens will comply with usability standards.
61	Access scripts with embedded ED PIN credential information are prohibited.
62	Procedures for key management (encryption) associated with the data repository exist for key generation, distribution, storage, use, destruction and archiving. The procedures associated with key management may be further strengthened particularly with segregation of responsibilities and maintenance of activity logs.
63	The ED PIN privacy policy statement or appropriate link will be displayed on all user facing pages. Additionally, this functionality will be identified as a U.S. Government system warning users about unauthorized access, punishment, etc. upon entering the ED PIN site.
64	The ED PIN site will meet the general requirements of Public Law 99-506 Reauthorization of the Rehabilitation Act of 1973, Section 508-Electronic Equipment Accessibility, October 1986; and Public Law 100-542 Telecommunication Accessibility Enhancement Act, October 1988.
64.1	Anonymous access to FAQ's associated with the functions and the use of the ED PIN system will be prominently displayed.
64.2	The ED PIN system will be capable of foreign language support (e.g., Spanish).
65	The ED PIN system will provide documented access interface alternatives for authentication functions in client systems. These access interface alternatives will follow applicable industry standards.
65.1	The preferred access interface will be identified by client systems during the

NO.	REQUIREMENT
	registration process.
65.2	Access interfaces, when developed in-house, will be available in Open Standard Languages (i.e. VB, C, C++, and Java, etc.).
66	The ED PIN system is the enterprise shared service for authentication of user identity.
66.1	The ED PIN credentials will support customer access to all borrower electronic services.
66.2	The ED PIN system design will be flexible to integrate with the federal e-gov e-authentication gateway.
67	The ED PIN system will possess capability for reliable date and time stamps for authentication requests.
67.1	Audit logs of authentication requests containing origin, results, date & time stamps will be maintained within the ED PIN system.
68	The ED PIN system will make First Name a mandatory field during individual user registration.
69	The ED PIN data will be maintained after initial registration through interfaces with users, FSA business processes and systems.
70	The ED PIN system will institute a formal registration process to authorize use of ED PIN functions by client systems. The formal process will be annual and documentation will be reviewed by the ED PIN business owner for compliance with requirements and standards.
71	Different implementations of electronic signatures will be documented.
72	Any change to user's identification data - SSN and DOB - will deactivate the current ED PIN associated with that user and require the generation of a new ED PIN. Changes to user's identification data may be initiated in any FSA business process related to the user.
72.1	SSN changes will require the issuance of a new ED PIN.
72.2	DOB changes will require an SSA match.
73	Users will be notified that any change to their identification data may result in the issuance of a new ED PIN. Changes to user's identification data may be the result of user initiated self service activity or from a registered client system.
73.1	An active ED PIN credential record cannot have a null First Name, Last Name, DOB, or SSN.
74	Duplicate SSNs will not be active in the ED PIN system.
75	A notification will be sent to the user if FSA determines that their ED PIN has been compromised.
75.1	Business rules for notifying customers in the advent of an ED PIN will be configurable.
76	Interim role-based ED PINs may be requested to support FAA authentication (e.g. those issued without SSA verification).
76.1	The ED PIN credentials issued to FAA's will be transitioned to the enterprise trading partner solution.
77	There will be segregation of responsibilities among ED PIN system administrators.

NO.	REQUIREMENT
77.1	The ED PIN system will support and enforce distinct access policies for different system administration functions.
78	The deactivation (lock-out) period (currently end of day) for the ED PIN will be configurable by the ED PIN system owner.
79	The total number of failed ED PIN authentication attempts by a user, regardless of session, will be configurable.
80	Internal access by authorized ED PIN system administrators will be logged and audited.
80.1	The event logging must be able to provide hooks for integrating in standard system monitoring architectures, facilities and tools (e.g. syslog). It must be configurable to support a choice of alert delivery channels such as e-mail, pagers, SNMP, etc.
81	The ED PIN reminder notification functionality will be available to FSA client systems.
81.1	Registered client systems seeking reminder notification functionality will document this requirement during the registration process.
82	The ED PIN reminder notification functionality will allow options for near real-time or batch communications.
82.1	The user will be notified of an ED PIN issuance.
83	The ED PIN system will be flexible enough to allow alphanumeric characters in the future.
83.1	Allow for a configurable PIN (current implementation based on a 4 character PIN).
84	All registered systems using the ED PIN authentication service will be notified of system problems, outage period and expected availability.
85	The ED PIN requirements and standards will be maintained and enforced.
86	End user facing screens for authentication will require all ED PIN access credentials and the screens will be consistent in the use of the credentials regardless of system.
87	All external access will be logged and the type of access will be based on authorized permission to use a particular ED PIN system function.
88	Host-based authentication to the ED PIN system is not permitted.
89	Certain ED PIN functions will utilize audit trail accountability. These functions will include any change to user information. The audit trail functionality will be configurable for number of changes.
89.1	The ED PIN system must be capable of accepting changes and corrections to all user data except SSN and DOB. Changes to SSN and DOB will be handled through a manual process.
90	Access to the ED PIN audit logs will be strictly controlled. There will be segregation of responsibility between groups that administer the access control function and those who administer the audit trail.
91	Confidentiality of audit trail information will be protected.
92	Audit trails will be reviewed and may utilize automated tools.
93	All ED PIN deactivations will be logged and reviewed by authorized personnel. Other appropriate security alerts will be defined in the ED PIN system security plan.
93.1	The event logging must be able to provide hooks for integrating in standard system

NO.	REQUIREMENT
	monitoring architectures, facilities and tools (e.g. syslog). It must be configurable to support a choice of alert delivery channels such as e-mail, pagers, SNMP, etc.
94	Data integrity problems (duplicate records, security violations, etc.) over a particular configurable threshold (e.g., .0001%) in the ED PIN user repository will be considered serious and will trigger a review. Availability of the ED PIN system during such audits will be decided by the ED PIN system owner.
95	Applicable demographic updates will be communicated among the ED PIN and FSA client systems.
95.1	Enterprise business rules associated with the SSIM process, once developed, will be incorporated into the re-engineering design.

3 Capacity Planning

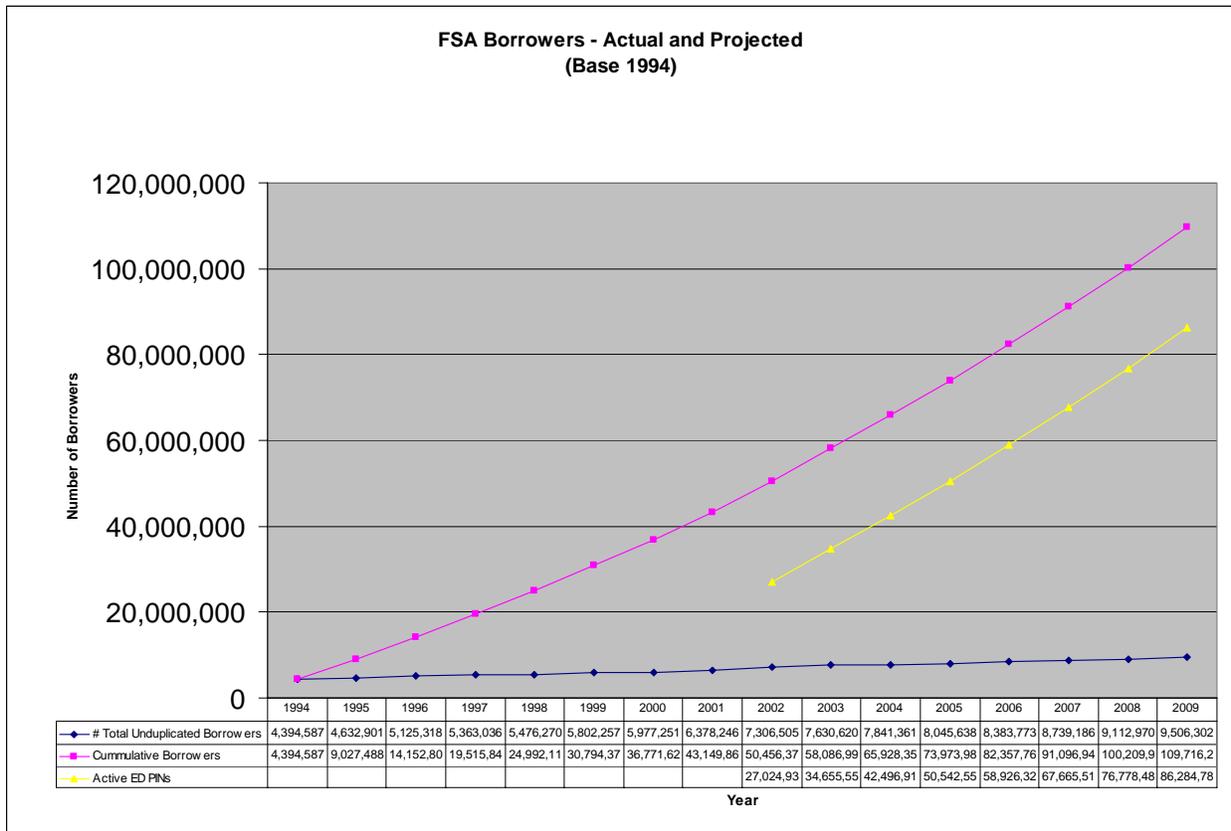
The capacity planning analysis is based on metrics from the ED PIN system most recent activity and projection for future usage. Estimates from previous years' activity were analyzed to project future capacity and performance considerations. Based on the results of the analysis, the capacity and utilization projections for the current system implementation are estimated through 2009. Many of the calculations and estimates are based on Student Borrower growth projections from the Student Loan Volume Tables – FY 2004 President's Budget⁷.

⁷ <http://www.ed.gov/offices/OUS/StudentLoanTables/index.html>

3.1 Number of Users

The following graph illustrates the projected growth of the Student Loan population and corresponding projected ED PIN growth. Included are tables for the average daily number of users and hits, as well as the estimated peak number of users and hits, and several significant calculations based on the peak number of users estimated.

Population figures were taken directly from the Student Loan Volume Tables – FY 2004 President's Budget. Active ED PIN projections are derived from actual 2002 metrics provided by the current CPS operations contractor (32,914,510 records in ED PIN in 2002 less 5,889,575 records in the system with no ED PIN = 27,024,935 Active ED PIN users).

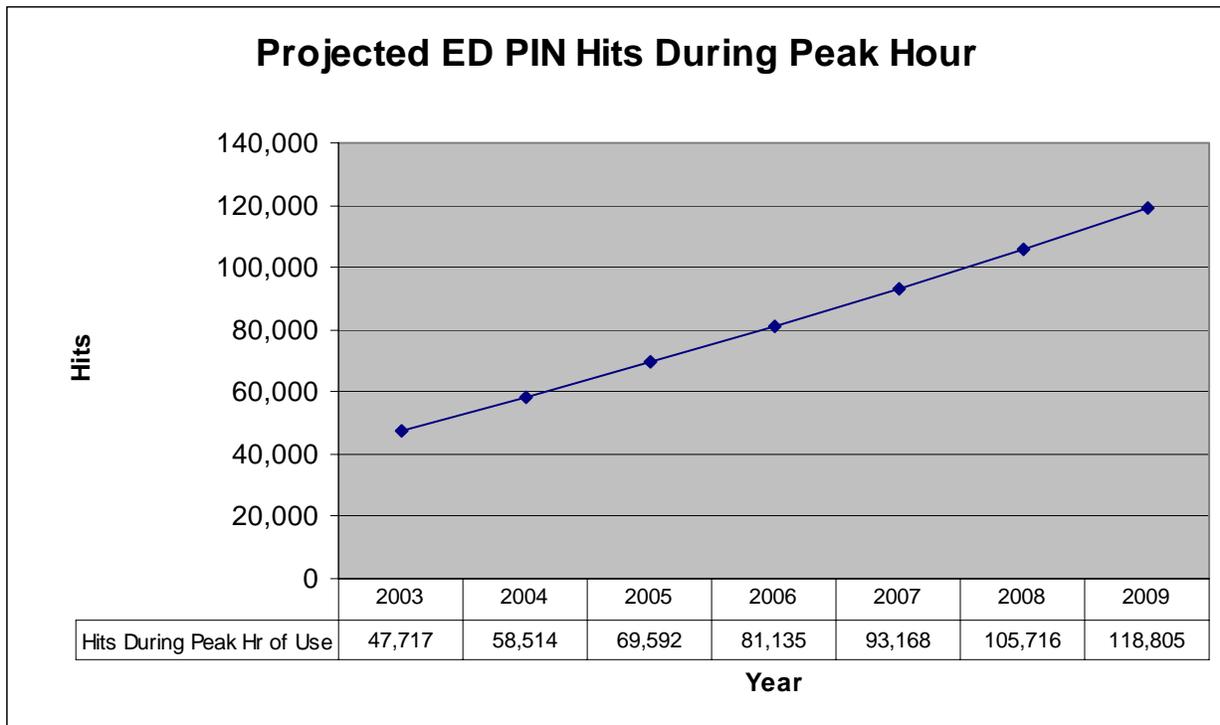


3.2 ED PIN Peak Usage Projections

The following information discusses the projected ED PIN usage based on the growth of the student loan population detailed above.

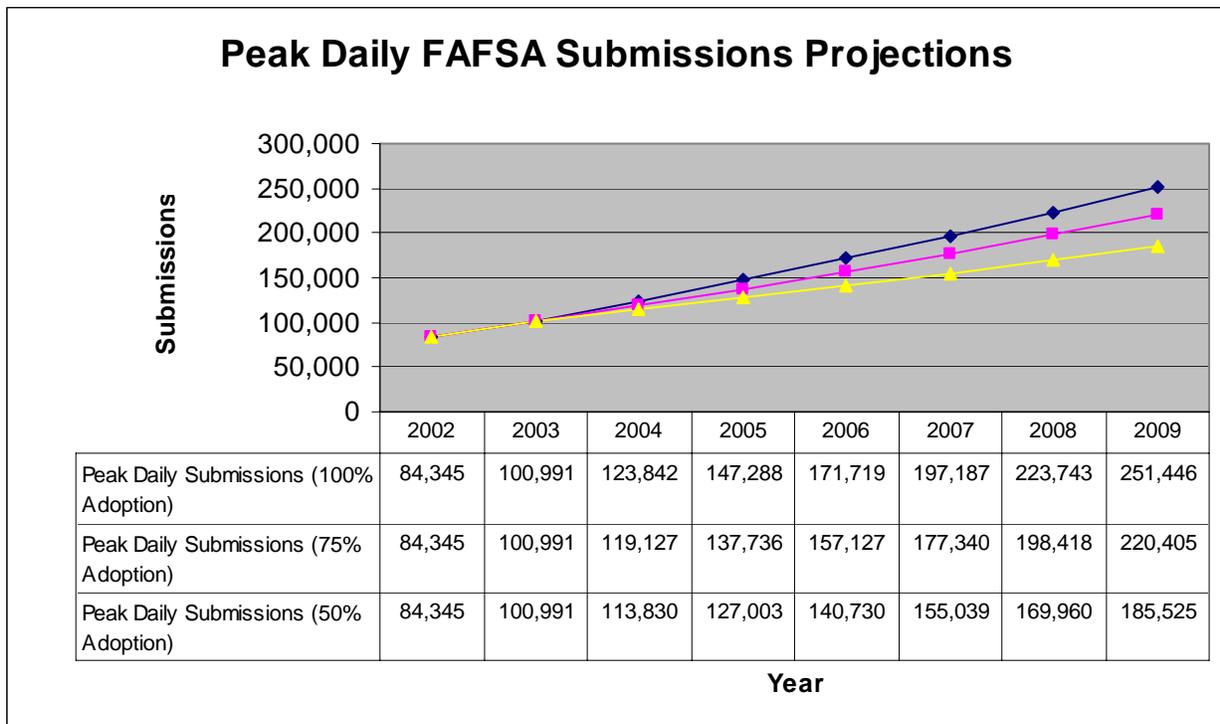
3.2.1 ED PIN Peak Usage Projection

The following estimates the peak usage to be experienced by the ED PIN system during the peak hour of yearly usage through 2009. Projections are based on actual ED PIN performance data provided by the CPS operations contractor for the period of December 2002 through July 2003. Projections through 2009 were derived by dividing the peak hourly usage for 2003 in terms of calls to the ED PIN DB (47,717 Hits) by the cumulative projected 2003 ED PIN records (34,655,555 Active ED PIN users). This ratio (0.31) is assumed constant and used to project the yearly maxima for hits/hour through 2009 based on the student loan populations mentioned above (e.g., 42,496,916 Active ED PIN Users projected in 2004 X 0.31 = 58,514 Projected Peak Hourly Usage in 2004).



3.2.2 Peak FAFSA Submission Projections

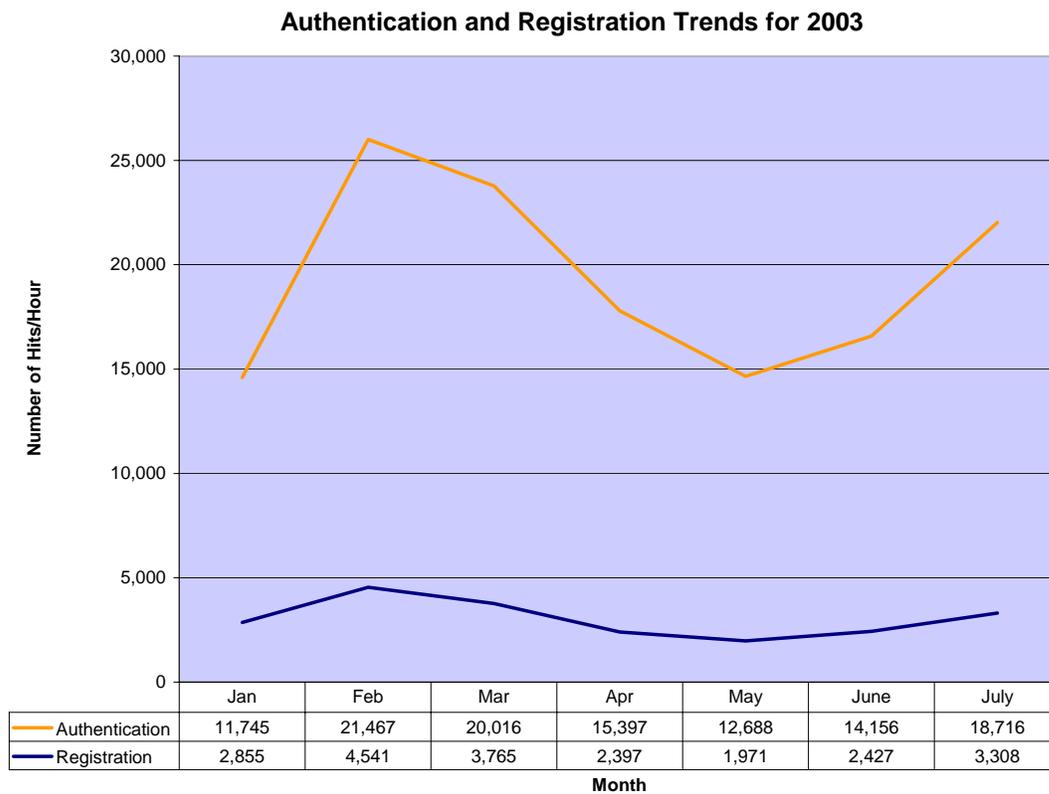
ED PIN usage is directly correlated to the FAFSA processing cycles. The majority of ED PIN usage occurs during the students' use of FAFSA on the Web and subsequent submission of the FAFSA application on-line. The FAFSA web application system and the ED PIN web system share the same Websphere ITA platform. The following graph illustrates the projected number of yearly peak electronic FAFSA submissions in one day through 2009. The projections were calculated by taking the ratio of actual FAFSA submission data in 2003 (100,991) to Active ED PIN users in 2003 (34,655,555 assuming 100% adoption rate, 32,747,900 assuming 75%, and 30,840,245 assuming 50%) and applying that ratio to projected Active ED PIN users through 2009. (e.g., 84,345 FAFSA submissions in 2002/27,024,935 Active ED PIN users in 2002*42,496,916 Projected Active ED PIN users in 2004 (assuming 100% adoption rate) = 132,633 projected electronic FAFSA submissions in 2004) Three scenarios were taken into consideration based on 100%, 75%, and 50% adoption rates of new ED PIN users. The actual number of peak daily FAFSA submissions is expected to be within this projected range.



3.3 ED PIN Usage Trends for 2003

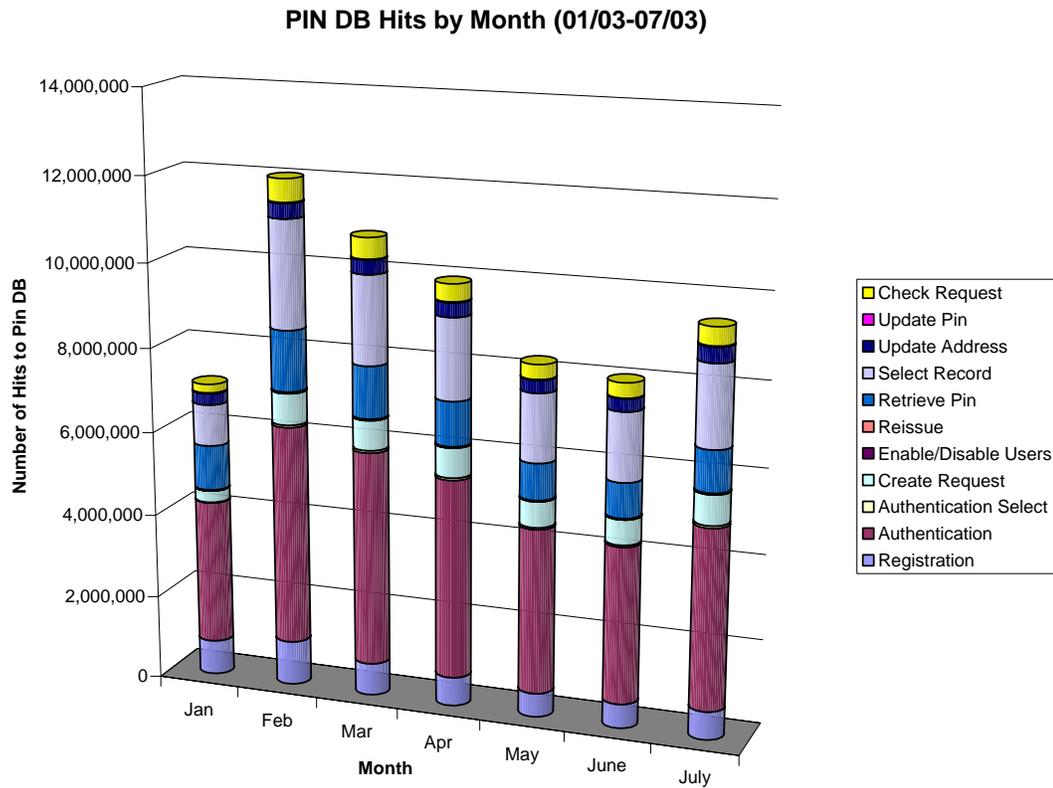
3.3.1 Period of Maximum Activity

The following graph illustrates trends in the usage of the ED PIN. Usage of the high volume business processes (Authentication and Registration) show annual peak occurring in the month of February. This coincides with the peak time for FAFSA application submissions during February 28th through March 3rd. It is anticipated that all peak volume projections will occur in this February-March time frame in the future. As expected, the graph clearly illustrates that ED PIN volumes are cyclical.



3.3.2 Usage Breakdown by Business Process

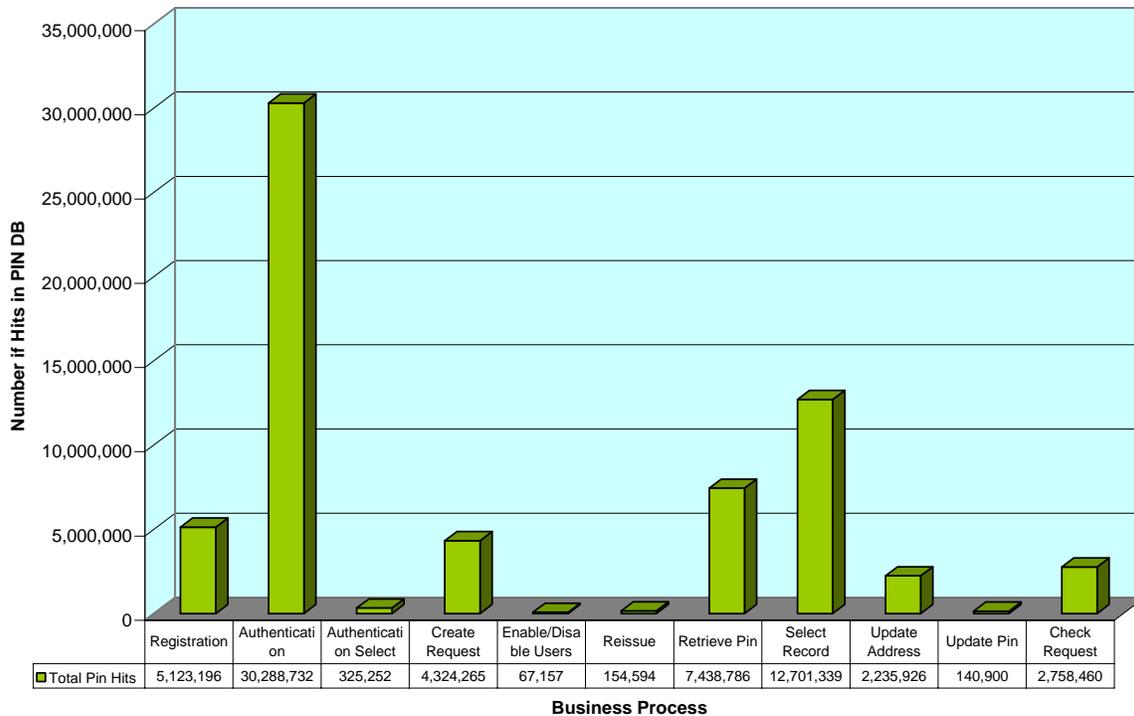
The following graph illustrates the total number of transactions in the ED PIN Database categorized by month. The data indicates that February and March are the time periods of heaviest usage and that Authentication is the most heavily utilized business function.



3.3.3 Cumulative ED PIN Hits for 2003 by Business Process

The following graph illustrates the total usage of the ED PIN DB categorized Business Process. Authentication, Registration, Select Record, and Retrieve ED PIN are the most commonly performed transactions on the ED PIN Database.

Total ED PIN DB Hits by Business Process (01/03 thru 07/03)



3.3.4 Monthly breakdown of Business Processes

The following table is a monthly breakdown of ED PIN Database usage categorized by Business Process.

Monthly ED PIN Hits from the ED PIN Database by Business Process (Jan 2003 - July 2003)

	Jan	Feb	Mar	Apr	May	June	July	Total
Registration	824,246	1,052,211	765,522	681,601	560,794	573,232	665,590	5,123,196
Authentication	3,417,511	5,203,847	5,078,227	4,721,596	3,900,872	3,701,466	4,265,213	30,288,732
Authentication Select	13,182	54,136	57,240	52,026	46,936	45,795	55,937	325,252
Create Request	278,829	746,355	705,017	700,465	603,385	587,209	703,005	4,324,265
Enable/Disable Users	5,648	12,451	10,830	10,047	9,073	8,633	10,475	67,157
Reissue	18,831	24,668	23,721	23,427	20,540	19,706	23,701	154,594
Retrieve ED PIN	1,064,642	1,441,993	1,232,944	1,044,991	858,764	820,756	974,696	7,438,786

	Jan	Feb	Mar	Apr	May	June	July	Total
Select Record	982,611	2,566,627	2,100,643	1,917,990	1,603,766	1,607,934	1,921,768	12,701,339
Update Address	272,239	353,164	330,408	334,069	293,607	292,338	360,101	2,235,926
Update ED PIN	19,962	21,821	20,969	20,834	18,602	17,722	20,990	140,900
Check Request	203,651	543,275	492,589	409,124	340,329	344,494	424,998	2,758,460

3.3.5 ED PIN Peak Hour Usage by Month

The following table illustrates the maximum number of hourly hits to the ED PIN Database in each month of the year 2003 (through July, 2003). The table shows similar trends between business processes from month to month.

Actual Peak Hits per Hour to ED PIN Database by Month - 2003

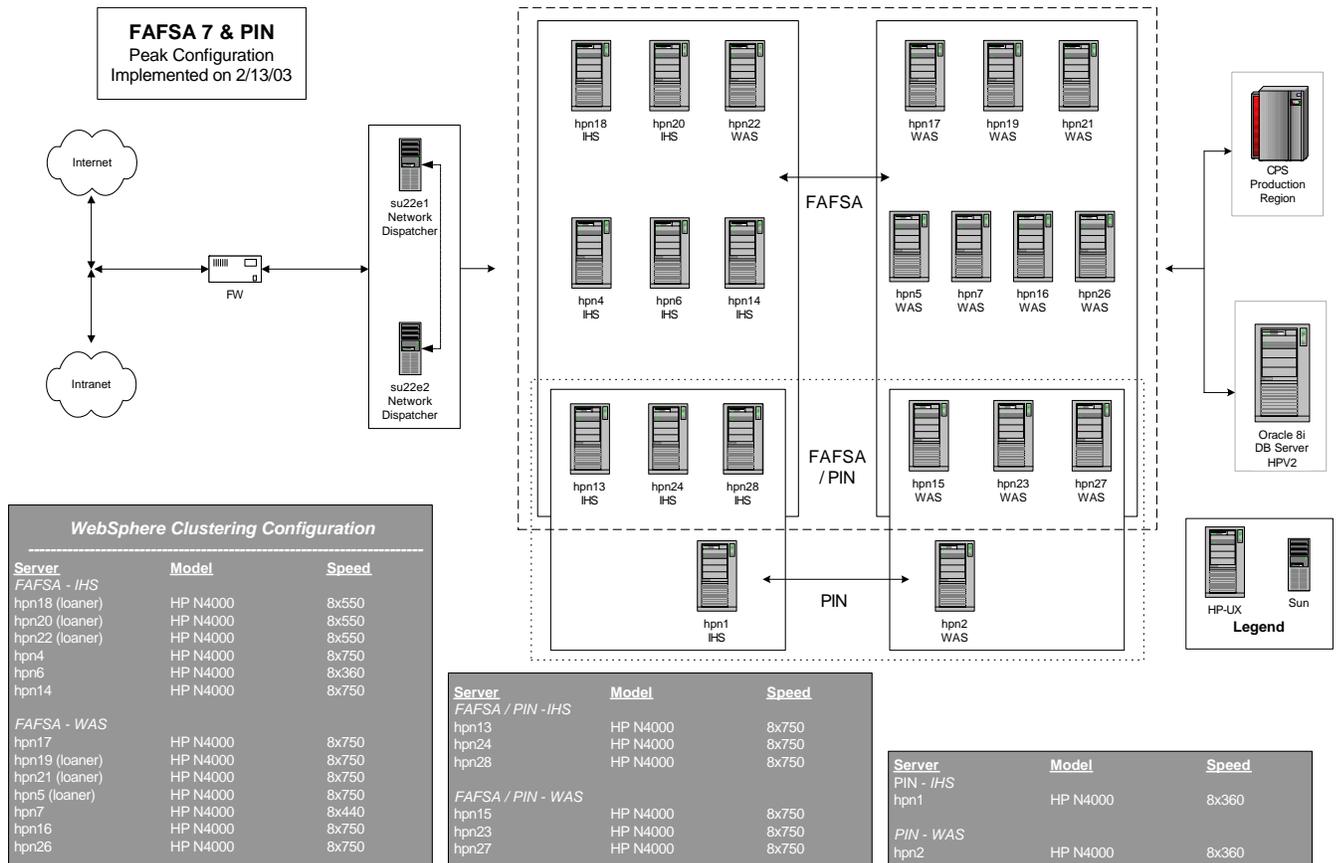
Business Process	Jan	Feb	Mar	Apr	May	June	July
High Volume Business Processes							
Registration	2,855	4,541	3,765	2,397	1,971	2,427	3,308
Authentication	11,745	21,467	20,016	15,397	12,688	14,156	18,716
Low Volume Business Processes							
Authentication Select	242	275	249	204	204	240	267
Create Request	1,795	3,066	2,792	2,483	2,349	2,635	3,573
Enable/Disable Users	63	70	62	55	66	61	62
Reissue	78	120	162	118	89	97	116
Retrieve ED PIN	3,714	7,398	6,607	4,083	3,277	3,139	3,870
Select Record	6,142	10,430	9,058	6,539	5,849	7,471	9,640
Update Address	1,128	1,468	1,359	1,193	1,154	1,305	1,852
Update ED PIN	87	118	117	93	86	87	100
Check Request	1,320	2,349	2,215	1,496	1,382	1,883	2,203

3.4 ED PIN Peak Period Performance Projections

3.4.1 FAFSA and ED PIN Integrated Architecture

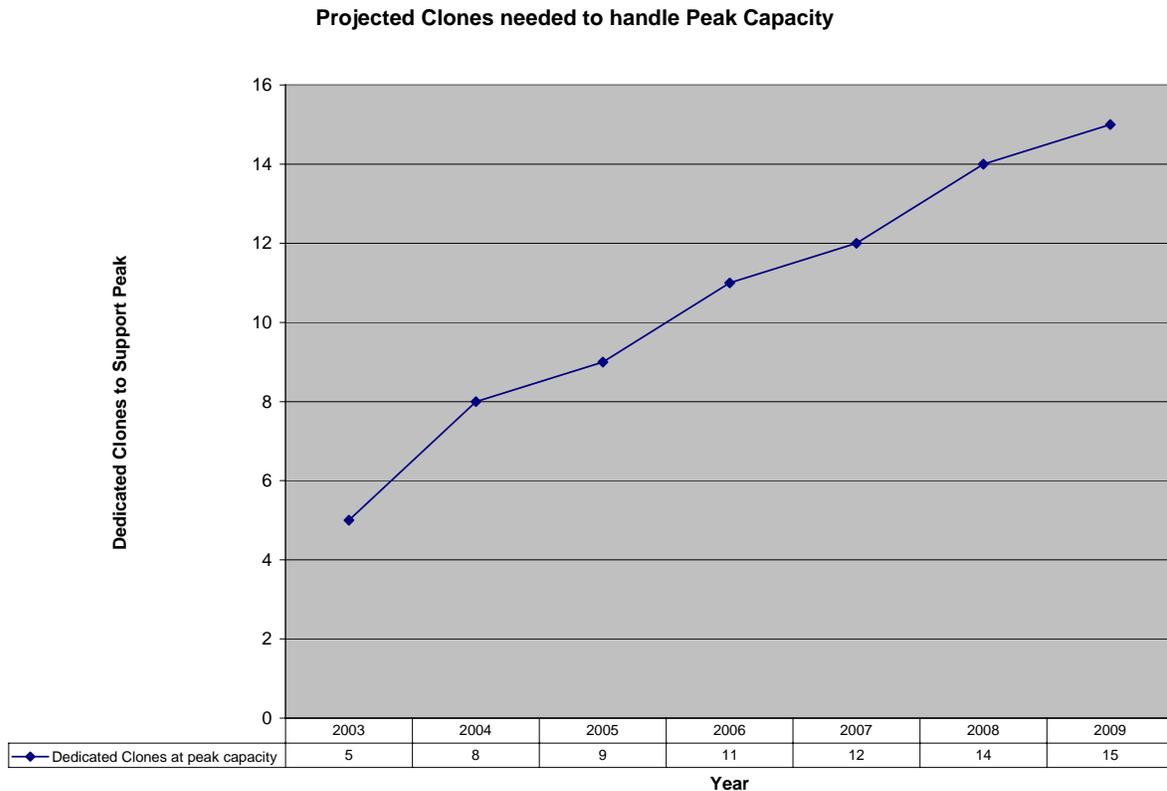
The ED PIN web architecture utilizes Akamai Web servers to host static information for the ED PIN. Web traffic requiring ED PIN database calls go through the ITA Web architecture. In 2003, the ED PIN was hosted on eight HP Web Application Servers. Out of those eight, two boxes were dedicated solely to ED PIN, while the other six shared services with FAFSA on the Web (FOTW) Application instances. In addition, FAFSA hosted ED PIN servlet instances that interfaced the ED PIN database directly.

Note: The vast majority of ED PIN system traffic due to FOTW went through this pathway. This activity of the ED PIN servlet on FOTW application instances was not accounted for specifically by any tracking device. More accurate and relevant could have been elicited from the web application usage had this ED PIN servlet activity been monitored. All the metrics associated with this analysis are focused around hits to the ED PIN Database itself. Capacity and performance considerations for the ED PIN system are accounted for in FOTW capacity planning, due to the technical and business interdependency of the two systems.



3.4.2 Performance Projections

The figure below represents the dedicated amount of processing capability needed to service the ED PIN through 2009. In 2003, ED PIN had five clones (an instance of the ED PIN application running on an application server) dedicated to support the peak period of activity (47,717 hits/hour). In addition, FAFSA application servers utilized an ED PIN servlet that allowed direct hits on the ED PIN Database. At non-peak periods (May through December), the ED PIN operates on two dedicated servers and two shared servers with FAFSA. Assuming servers with similar processing capability (8X360 MHz CPU); this ratio (47,717 hits per 5 clones) was used to project the number of clones needed to handle future peak hourly usage. The projected peak hourly usage figures (derived in section 3.2) were multiplied by the 2003 ratio to obtain the yearly estimates. In addition, estimations include 20% CPU processing contingency based on performance degradation as activity increases. (e.g., 2004 clone estimation (8) = peak hourly usage projection (58,514 hits)*20 %*(dedicated clones used in 2002 (5)/hits in peak hourly usage (47,717))).

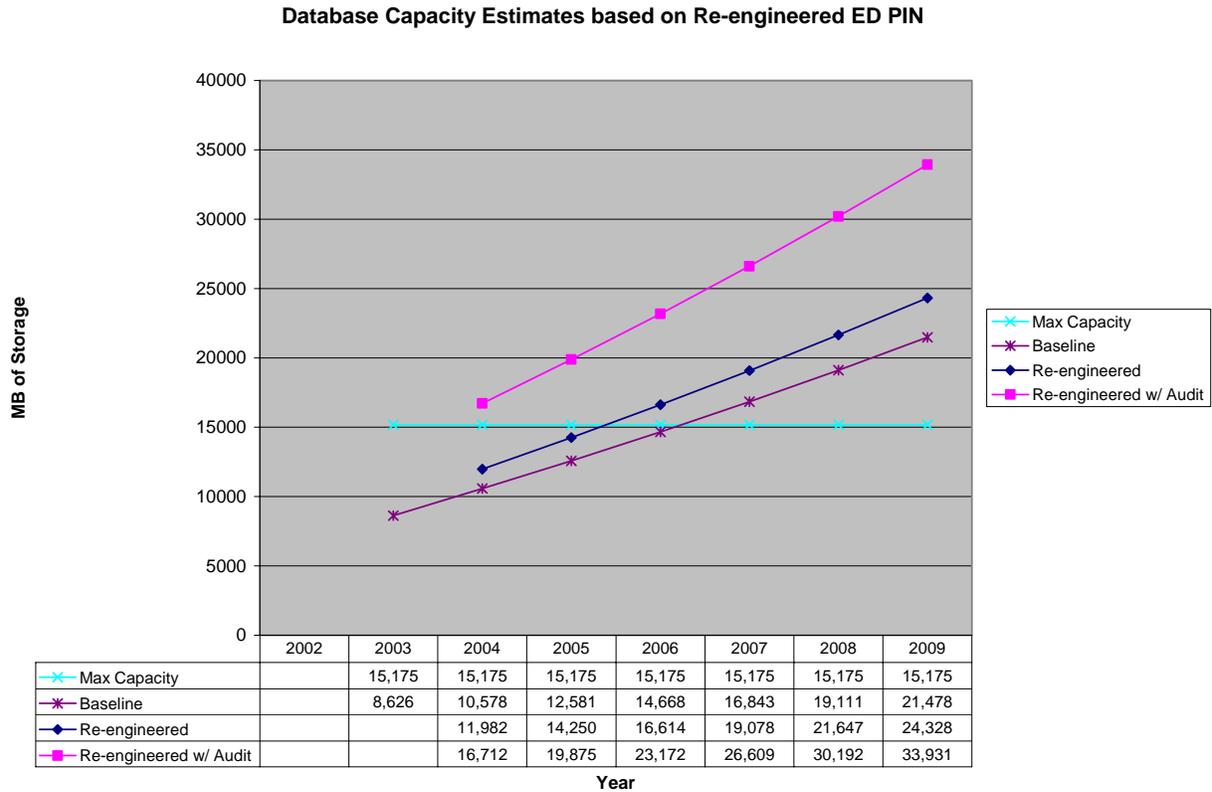


Data regarding ED PIN Database (provided by the FSA Virtual Data Center on a monthly basis) indicates an approximately 3% average CPU utilization on the ED PIN Database. ED PIN usage is expected to triple by 2009 (27 million active ED PINs in 2002 to 86 million active ED PINs in 2009). Should the population double, CPU utilization was calculated to be 6.6%. The calculated CPU utilization was 10.2% for a tripling of the user population. (Assuming a 20% CPU utilization contingency for every doubling of the population (e.g., Doubling of the population = $2(3\% \text{ current CPU utilization}) + 1(20\% \text{ contingency} * 3\% \text{ utilization}) = 6.6\% \text{ CPU utilization}$).

3.5 ED PIN Database Considerations

This subsection provides a related analysis for the ED PIN database storage capacity through 2009. Growth Projections discussed previously were applied to the current ED PIN database metrics provided by the FSA Virtual Data Center (8,626 MB used of an allocated 15,175MB as of 9/23/03). The projections are shown in the “Baseline” figures of the graph. The current procurement of database capacity is also displayed as “Max Capacity”. The data model for the re-engineered ED PIN will be different requiring a series of additional data capacity considerations. Two of the data capacity considerations for the re-engineered ED PIN are history tracking and audit log/report creation. The “re-engineered” ED PIN data represents the projected database storage usage if demographic history is tracked. History tracking estimates were derived from sizing figures provided by the current CPS Operations contractor. An estimated 6.3 million demographic updates were made on ED PIN, CPS, and DL from January to July of 2003. Rough estimates are that recording demographic history will require an additional 106 bytes of storage per record. This actual data and estimation was used to create an estimate of database storage requirements for this data element of the re-engineered ED PIN and added to the current storage capacity for an overall storage estimate. These estimates were then projected out through 2009. A similar estimate was made for the data estimates for audit capability. The “re-engineered with audit” data represents the approximate database storage usage if authorization and e-signatures audit logs were included in the re-engineered ED PIN. Because the specific audit logs and reports have not been defined, a realistic estimate cannot be calculated at this time. However, authorization and e-signature audits will be a significant data capacity element of the re-engineered ED PIN. The CPS operations contractor estimates 30 million authorization and e-sign requests were made on ED PIN from January to July of 2003. Rough estimates are that an audit record for such a request would be 75 bytes. This actual data was used to create an estimate of database storage requirements for this element of the re-engineered ED PIN and added to the initial re-engineered ED PIN estimate for an overall storage estimate. These estimates were then projected out through 2009.

*Note: These estimates are only examples used to give an idea of the database impacts to the re-engineered ED PIN. These estimates also assume a 2004 implementation. In addition, the data only represents the production environment. A thorough analysis should be performed when the data model is clearly defined. These estimates are based on interaction with existing client systems. This estimate should be re-evaluated as additional systems begin to use the ED PIN.



The graph indicates that the average growth rate for the re-engineered ED PIN with audit capability is approximately 2,870 MB annually. Based on the growth projections, the current SLA for ED PIN database operational capacity will be exceeded in 2005. The data indicates that the current ED PIN database resources would not support the re-engineered ED PIN. At peak usage in 2009, the estimates are on the order of 35 GBs. Even if the data requirement is doubled, the ability to store ED PIN data is not an issue for current technology. Annually, the re-engineered ED PIN production database size is projected to require 40 to 60 GBs of storage for 2004 and 2005. Database sizing estimates should be re-evaluated at least annually and as the data model and detail design for the re-engineered ED PIN is developed.

3.6 Summary of Capacity Findings

- The data indicates that student borrower populations will significantly increase over the next five years to over 109,000,000 by 2009 (based on projections in section 3.1).
- The usage patterns demonstrate cyclical ED PIN volumes that reach their peak during the February-March timeframe of the year.
- Authorizations and Registration were found to be the most heavily used business functions on the ED PIN system.
- The findings indicate that the current technical architecture is scalable to support ED PIN growth for the current implementation of the ED PIN system. This is made possible by the hosting of ED PIN on the ITA infrastructure and the co-existence with FOTW that suggests a scalable architecture.
- Collective projections made by various FSA client systems for hourly transaction volumes by business process (See Appendix C) significantly differed from the actual results (purple shaded sections of Appendix C). In addition, activity of the ED PIN servlet on FOTW application instances was not accounted for specifically by any tracking device. More accurate and relevant information (and in turn projections) could have been elicited for the ED PIN system had these activities been monitored. This suggests the need for more robust tracking and auditing capabilities for the ED PIN system in the future.
- Our analysis projects that currently acquired ED PIN database resources (15,175 MB of storage) will be sufficient to safely support the current ED PIN through FY04, but will not be sufficient to support the re-engineered ED PIN storage requirements. Annually, the re-engineered ED PIN production database size is projected to require 40 to 60 GBs of storage for 2004 and 2005. Database sizing estimates should be re-evaluated at least annually and as the data model and detail design for the re-engineered ED PIN is developed.

4 Conclusions

The technical architecture upgrade analysis phase of the ED PIN Re-Engineering initiative examined the ED PIN from the perspective of establishing it as an enterprise authentication service. FSA has a business need to have a mechanism for authenticating customers seeking services via web-based products. FSA also has a business need to provide an electronic signature option to its customers in lieu of paper processes thereby supporting and implementing a completely paperless process. Since its inception in 1997, the ED PIN has become the user authentication source for 8 FSA business applications that include:

- FAFSA on the Web
- NSLDS
- e-Campus Based
- Direct Loan Servicing
- Direct Loan Consolidation
- FAA Access Online
- STAN, and
- ED PIN.

In addition to the business systems listed above, the ED PIN is being considered for Common Services for Borrowers (CSB) and E-Gov initiatives. Use of the ED PIN for authenticating E-Servicing IVR customers may also be a potential future function. It is clear that the ED PIN is a successful implementation for customer authentication with over 34 million records in its repository. The ED PIN evolution during the past 7 years, however, requires certain changes to ensure its continued foundation as an authentication and electronic signature source.

Maintaining the integrity of the ED PIN data store associated with individual authentication should be the top priority for its continued success. This implies that verification of user identity is an important first step in the issuance of the ED PIN credential. Data matching with the SSA is a strong method for verification that includes the SSN, name and date of birth of an applicant and should definitely be continued. While sources for verification of other demographic information (e.g., address) are also commercially available, the additional verification does not appear to be necessary. However, the capability to perform additional, or supplemental verification at the enterprise level, is needed to enhance the integrity of user data when necessary and prevent unauthorized authentication to FSA application systems. At the enterprise level, FSA's implementation of the SSIM process will help maintain ED PIN data integrity. The re-engineering design should include the capability for using other verification sources such as the consolidated and standardized federal government's watch list structures and policies currently under development by the Department of Homeland Security.

Business functions performed by users of the ED PIN that do not necessitate revealing personal information should not use the ED PIN as an authentication credential. This implies that FAAs and trading partners currently using the ED PIN to authenticate themselves for access to FAA

Access Online and e-Campus Based should be transitioned off the ED PIN. Specific recommendations from the enrollment and access management initiative currently underway should address the appropriate credentials for this user group.

FSA's implementation of electronic signature functionality based on the SSA-matched ED PIN credential is appropriate and complies with the e-sign legislation. To maintain integrity of an electronic signature and its relationship to an individual it is important for FSA to only allow a single ED PIN credential per user. Authenticity of electronic signatures associated with multiple ED PIN identities should not be permitted and compromises the long term integrity of the ED PIN.

A process for permitting electronic access to FSA borrower records without social security numbers, i.e., records generated with pseudo SSNs in FSA business systems, should also be developed. While the number of such customers and the volume of transactions are relatively minimal, a solution that encompasses the entire borrower community is necessary. ED PINs may be issued to customers with pseudo SSNs as long as the credential is generated from FSA systems possessing those records. However, such issuance should be controlled within the ED PIN processes by only permitting FSA business systems with existing pseudo SSN records to process an ED PIN registration application; direct application by pseudo SSN customers should not be permitted. Customers with ED PINs issued without an SSA match (e.g., pseudo SSN) should not have their credentials enabled for electronic signature functions.

In its implementation, the ED PIN needs to continue to be easy to use while complying with federal and FSA policies and standards for usability, security, privacy, authentication and electronic signature. Both the business and technical requirements have been updated as part of this effort. A capacity analysis related to the current ED PIN system infrastructure was also performed during this initiative. There do not appear to be any critical issues with infrastructure capacity for the ED PIN since it is hosted on the FSA integrated technical architecture that shares infrastructure with FAFSA on the Web. Both FAFSA on the Web and the ED PIN have cyclical and related transaction cycles and the technical architecture scales well.

The development of standard and reusable services associated with the five ED PIN enterprise functions need to be part of the re-engineered process. These services include:

- Identification
- Registration
- Access
- Self-Service, and
- Administration.

The re-engineered solution should possess identification components for both individual users and systems (ED PIN authentication clients) thereby possessing the capability to prevent unauthorized use of the ED PIN system. While the identification component for individual users is currently implemented, the process for client systems will need to be developed during

the re-engineering effort. The registration process should add flexibility for supplemental individual verification of users (in addition to SSA verification match) as part of the re-engineering design and a formalized annual process for registration of client systems should be implemented. Functionality within the registration process should distinguish between individuals verified through the SSA match or other sources. This functionality will allow FSA the capability to service its entire student customer base including individuals without social security numbers (e.g., Pacific Islanders).

The access process should separate the distinct functionality associated with authentication and electronic signature. Authentication should be implemented for both individual users and client systems as part of any transaction request to the ED PIN system. Self-service functionality can be enhanced to encourage increased use of the ED PIN while minimizing customer service contact. And finally, the administration process should be strengthened as part of the re-engineering effort to include standard management reports as well as intelligent alerts associated with potential security and privacy threats.

New or changed features associated with the ED PIN re-engineering effort include:

- A focus on data integrity of the ED PIN as an authentication credential
- Separate authentication and electronic signature functions
- Registration and verification of client systems with annual refresh cycle
- Alerts and management reports
- Singular and unique user record in ED PIN data repository
- Enhanced user self-service capabilities, and
- Standard, reusable services for identification, registration, access, self-service and administration.

Re-engineering activities to transition from the current ED PIN implementation will require planning and integration to ensure continued service to customers. The planning and integration activities should include a Data Integrity Plan to ensure there are no duplicate records. The planning effort will also need to address development of a formal annual process for client systems. Management reports and alert criteria need to be included as part of the detailed design. The interface with client systems will need to be upgraded to include both a standard process as well as technical specifications to handle batch and real-time requests.

Recommendations for the re-engineered ED PIN solution include design and deployment of a

Individuals	IDENTIFICATION	Systems
Individuals	REGISTRATION	Systems
Authentication - Individual - System	ACCESS	Electronic Signature
SELF-SERVICE		
Alerts	ADMINISTRATION	Management Reports

set of standard and reusable components for identification, registration, access, self-service, and administration services. The re-engineered solution should possess identification components for both individual users and systems (ED PIN authentication clients) thereby possessing the capability to prevent



unauthorized use of the ED PIN system by either users or systems. The ED PIN system should be used for the borrower community only (i.e., students and parents). The ED PIN is not a suitable credential for trading partners including FAAs. A plan to transition FAAs to a different authentication credential should be developed as part of the Identity and Access Management (I&AM) initiative. The registration process should continue to rely on SSA verification of individual information but also possess the flexibility for supplemental verifications such as those with terrorist, prisoner and other sources. The registration process associated with client systems should also be formalized as an annual activity to ensure all requirements are known and tested. Functionality within the registration process should distinguish between individuals verified through the SSA match and other sources. This functionality will allow FSA the capability to service its entire student customer base including individuals without social security numbers (e.g., Pacific Islanders).

The access process should separate the distinct functionality associated with authentication and electronic signature. Authentication should be implemented for both individual users and client systems as part of any transaction request to the ED PIN system. Self-service functionality should be enhanced to encourage increased use of the ED PIN while minimizing help desk contact. And finally, the administration process should be strengthened as part of the re-engineering effort to include standard management reports as well as intelligent alerts associated with potential security and privacy threats.

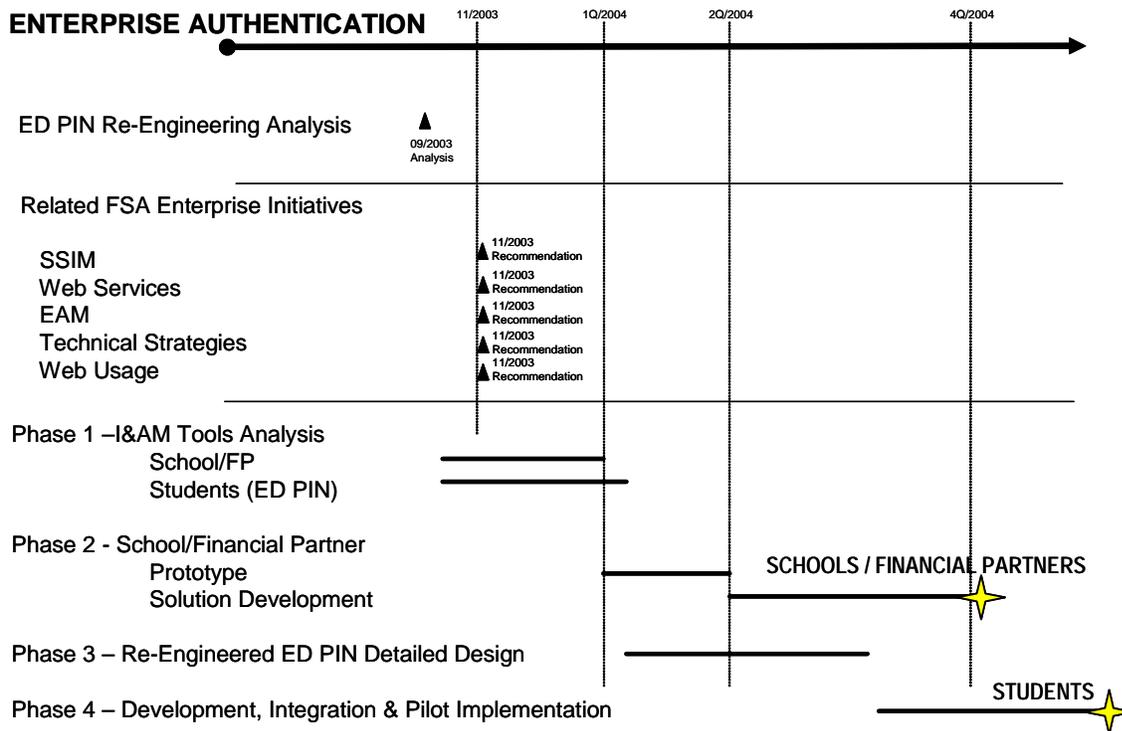
A 4-phased approach is recommended for the ED PIN re-engineering of processes and supporting systems to integrate with an enterprise authentication solution. Phase 2 does not directly involve the ED PIN system. The recommendations include:

- Phase 1 – Tools Analysis (Joint with ED PIN and School/Financial Partners)
- Phase 2 – School/Financial Partners Prototype and Solution
- Phase 3 – Re-Engineered ED PIN Detailed Design, and
- Phase 4 – Development, Integration and Pilot Implementation of re-engineered ED PIN system.

The 4-phased approach is recommended for establishing an FSA-wide enterprise authentication solution that includes both trading partners (schools and financial partners) and students. The 4-phased approach incorporates decision milestones at the end of each phase to (1) ensure that goals for each phase are met and (2) provide an opportunity for FSA executive decisions in light of other enterprise priorities. The goal for Phase 1, Tools Analysis, are to participate in a joint tools analysis with the I&AM initiative and conduct a tools analysis to decide whether a commercial off the shelf (COTS) solution is cost beneficial or to continue development of an in-house solution. The tools analysis phase with the I&AM effort should attempt to ascertain whether a single enterprise solution can support both the trading partner and student business requirements. While the trading partner solution is prototyped, FSA can transition to Phase 2, Detailed Design. The goals for Phase 2 are to prototype and implement an enterprise solution for schools and financial partners. The goals of Phase 3 are to leverage lessons learned during phase 2 to re-engineer and design the enterprise level processes for the 5 business functions associated with the ED PIN. This phase should leverage lessons learned from the I&AM

prototype and incorporate best practices into the design. Phase 4, Development, Integration and Pilot Implementation, can then develop the student focused ED PIN authentication service as an extension to, or separate instance of, the I&AM schools / financial partners implementation.

The recommendations for a re-engineered ED PIN solution result in a comprehensive enterprise authentication solution for borrowers that can be leverage across all appropriate business processes. Such a solution will require focused communications with current users (both client systems and trading partners) to ensure transition activities are completed successfully.



The requirements analyzed in this document provide system, infrastructure and process information in support of an enterprise solution to meet the complete set of FSA’s business requirements. These requirements have been analyzed in coordination with the FSA Security and Privacy Technical Architecture Vision. Activities during this phase also focused on close coordination with FSA’s ongoing Data Strategy initiative particularly for the enterprise direction related to standard student identification method (SSIM), web services, enrollment and access management, technical strategies, web usage and integrated technical architecture. The technical requirements also incorporate Federal standards and policy guidance for e-authentication. The ED PIN should undergo a credential assessment to ascertain its specific level related to the e-authentication guidance.

The capacity analysis utilized actual and projected Title IV program applicants to determine hardware infrastructure needs. The ED PIN system does not have any critical infrastructure requirements beyond its current implementation on the FSA integrated technical architecture



for the 2004 - 2005 school year. The capacity analysis provides infrastructure recommendations for both peak and off-peak transaction processing requirements. ED PIN transactions are expected to grow at an annual rate of approximately 25% for the next 6 years. Capacity projections will need to be re-examined upon completion of the re-engineered ED PIN system.

APPENDIX A – REFERENCES

1. CPS Web Applications 2003-2004 Requirements Detail Design Document 34CL-601 (PIN Web Site) thru Addendum 5.
2. The FSA PIN Overview.
3. CPS Web Applications 2003-2004 Requirements Detail Design Document 34CL-602 (PIN Application Programming Interface) thru Addendum 1.
4. CPS Web Applications 2003-2004 Requirements Detail Design Document 34CL-616 (PIN Application/PIN Address Correction) thru Addendum 1.
5. Report of PIN executions (Dec – March) for Update PIN, Update Address, Enable/Disable, Insert New PIN User, Reissue, Retrieve PIN, Select Record (no Dec data), Create Request (no Dec data), Check Request (no Dec data), and Authenticate.
6. CPS Web Applications 2003-2004 Requirements Detail Design Document 34CL-610 Addendum #3.
7. FAFSA PIN Uses Document.
8. STAN Functional Specifications document, version 2.3, dated 2/14/2003, Tracker log #185.
9. National Institute of Standards and Technology. *An Introduction to Computer Security: The NIST Handbook*. Special Publication 800-12. 1995
10. National Institute of Standards and Technology. *Minimum Security Requirements for Multi-User Operating Systems*. NISTIR 5153. March 1993.
11. Privacy Working Group, Information Policy Committee, Information Infrastructure Task Force. *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information*. June 6, 1995.
12. U.S. Department of Education Strategic Plan 2002 – 2007.
13. National Institute of Standards and Technology. *Guidelines for the Security Certification and Accreditation of Federal Information Technology System*. Initial Public Draft, Version 1.0, October 2002.
14. E-Authentication Levels – Working Draft, OMB, March 2003.
15. FSA Proposed Business Justification. ED PIN Re-Engineering Analysis. March, 2003.
16. Generally Accepted System Security Principles (GASSP), I²SF, Version 2.0. June 1999.
17. FSA Integration Partner Deliverable 124.1.3, Security and Privacy Architecture Specification. May 2003.
18. FSA Integration Partner Deliverable 123.1.22, CSID (*renamed to SSIM*) High Level Design. May 2003.
19. FSA Integration Partner Deliverable 131.1.2, Updated ED PIN Requirements and Standards, August 2003.
20. Common Criteria for Information Technology Security Evaluation (ISO/IEC Standard 15408), version 2.1, August 1999.
21. Identity Theft: Greater Awareness and Use of Existing Data Are Needed. GAO-02-766 June 28, 2002.
22. Identity Theft: Prevalence and Cost Appear to be Growing. GAO-02-363 March 2002.
23. Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing. GAO-03-322 April 2003.

24. ID Theft: When Bad Things Happen to Your Good Name. Federal Trade Commission.
September 2002.

APPENDIX B – DEFINITION OF TERMS

Acceptable Risk – A concern that is acceptable to responsible management, due to the cost and magnitude of implementing security controls.

Accountability – Property that allows the ability to identify, verify, and trace system entities as well as changes in their status. Accountability is considered to include authenticity and non-repudiation.

Adequate Security – Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

Authentication – Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual’s authorization to receive specific categories of information.

Availability – Assurance that information, services, and IT system resources are accessible to authorized users and/or system-related processes on a timely and reliable basis and are protected from denial of service.

Component – An IT assembly, or part thereof, that is essential to the operation of some larger IT assembly and is an immediate subdivision of the IT assembly to which it belongs, (e.g., a trusted guard, biometrics device, or firewall would be a component of a computer system).

Confidentiality – Assurance that information in an IT system is not disclosed to unauthorized persons, processes, or devices.

Configuration Management – A family of security controls in the management class dealing with the control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of an IT system.

Contingency Planning – A family of security controls in the operations class dealing with emergency response, backup operations, and post-disaster recovery for an IT system, to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation.

Criticality/Sensitivity – A measure of the importance and nature of the information processed, stored, and transmitted by the IT system to the organization’s mission and day-to-day operations.

Data Integrity – Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered or destroyed.

Designated Approving Authority – Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated accrediting authority and delegated accrediting authority.

Developer – The organization or individual that develops the IT system.

Environment – Aggregate of external procedures, conditions, and objects affecting the development, operation and maintenance of an IT system.

Exposure – A measure of the potential risk to an IT system from both external and internal threats.

External System Exposure – Relates to: (1) the method by which users access the system, (e.g., dedicated connection, intranet connection, Internet connection, wireless network), (2)

the existence of backend connections to the system and to what the backend systems are connected, and (3) the number of users that access the system.

Firmware – Program recorded in permanent or semi permanent computer memory.

Identification – The process of ascertaining an individual’s identity or confirming that the purported identity is correct. Identification relies on one or more of three factors: something an individual has, something an individual knows, and something an individual is (such as signature or biometric attribute).

Identification and Authentication – A family of security controls in the technical class dealing with ensuring that users are individually authenticated via passwords, tokens, or other devices, and that access controls to the IT system are enforcing segregation of duties.

Individual Accountability – Requires individual users to be held accountable for their actions after being notified of the rules of behavior in the use of the system and the penalties associated with the violation of those rules.

IT Security – Information operations protect and defend information and IT systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of IT systems by incorporating protection, detection and reaction capabilities.

IT System – The set of agency information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Categories of IT systems are major applications and general support systems.

Integrity – Assurance that information in an IT system is protected from unauthorized, unanticipated, or unintentional modification or destruction. System integrity also addresses the quality of an IT system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data.

Internal System Exposure – Relates to the types of individuals that have authorization to access the system and the information the system stores, processes, and transmits. It includes such items as individual security background assurances and/or clearance levels, access approvals, and need-to-know.

Logical Access – A family of security controls in the technical class dealing with ensuring that logical access controls on the IT system restrict users to authorized transactions and functions.

Non-Repudiation – Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender’s identity, so neither can later deny having processed the data.

Operational Controls – Controls that address security mechanisms primarily implemented and executed by people (as opposed to systems).

Residual Risk – Portion of risk remaining after security controls have been applied.

Risk – The net mission impact considering: (1) the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular IT system vulnerability and (2) the resulting impact if this should occur. IT system-related risks arise from legal liability or mission loss due to: (1) unauthorized (malicious or accidental) disclosure, modification, or destruction of information, (2) unintentional errors and omissions, (3) IT

disruptions due to natural or man-made disasters, and (4) failure to exercise due care and diligence in the implementation and operation of the IT system.

Risk Assessment - The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of risk management and synonymous with risk analysis.

Subsystem - A major subdivision or component of an IT system consisting of hardware/software/firmware that performs a specific function.

System - A generic term used for brevity to mean either a major application or a general support system.

System and Data Integrity - A family of security controls in the operations class dealing with the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data.

User - Person or process authorized to access an IT system.

Vulnerability - A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the systems security policy.

APPENDIX C: ED PIN Transactions per hour at peak (Projected Volume) January 2002 - April 2003

Future Applications/Additional Growth	Business Process	Pin DB via website	Pin DB Directly	Peak hour range	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	June	July
Direct Loan Servicing Web Site including EBPP/EC	Registration (also includes eCRM)	Batch Process Flex w/ time of the day		flexible	5,000	4,900	4,800	4,800	4,800	4,800	4,800	4,800	4,800	4,800	4,800	4,800	5500	5390	5280				
	Authentication	X		12-2pm	1,250	1,758	1,065	5,692	5,680	5,630	5,883	5,848	5,622	5,711	5,754	5,494	9375	8626	9478				
eCRM VRU Pin	Authentication		X	12-2pm	1,044	999	951	753	736	765	898	840	682	807	800	774	1149	1099	1046				
Consistent Answers	Registration		X	N/A																			
	Authentication														524	600	733	733	600				
Students Portal Release 2 (traffic redirection)	Registration	N/A	N/A	N/A																			
	Authentication																						
STAN - Perkins (only additional growth) **	Registration		X	N/A				2	2	3	6	6	4	2	2	2							
	Authentication							13	16	23	46	46	30	13	13	13							
STAN - FFEL (only increase traffic) **	Registration		X	N/A				0	0	0	1	2	3	0	0	0							
	Authentication							0	0	2	7	20	27	3	0	0							
STAN - Direct Loan Consolidation (only increase traffic)**	Registration		X	N/A				0	0	0	1	4	5	4	2	2							
	Authentication							1	0	3	12	33	38	30	19	15							
STAN - Direct Loan Origination (only increase traffic) **	Registration		X	N/A				0	4	8	16	32	14	2	0	0							
	Authentication							0	33	67	133	267	117	17	0	0							
Single sign-on	Registration	N/A	N/A	N/A																			
	Authentication																						
FAFSA on the Web 7.0 /Student Access/FAA Access	Registration		X	4-7pm																			
	Authentication																						
Direct Loan Consolidation (only additional growth)**	Registration	N/A	N/A	N/A				0	0	0	1	4	5	4	2	2							
	Authentication							1	0	3	12	33	38	30	19	15							
Direct Loan Origination (only additional growth)**	Registration	X		1-5pm					0	1	3	5	3	2	2	0	0	0	0				
	Authentication								2	8	25	45	25	16	13	4	4	4	4				
Total Projected transactions	Registration				0	0	0	2	6	13	28	53	33	13	70	78	87	87	72	0			

Future Applications/Additional Growth	Business Process	Pin DB via website	Pin DB Directly	Peak hour range	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	June	July
for future applications																							
	Authentication				1,044	999	951	769	788	870	1,134	1,283	956	915	1,389	1,422	1,886	1,836	1,650	0			
High Volume Business Processes																							
Total Existing Hits(peak hour) from the Pin Database	Registration				N/A	2,306	1,688	1,034	1,182	973	1,311	1,477	964	N/A	N/A	1,362	2,855	4,541	3,765	2,397	1,971	2,427	3,308
	Authentication				N/A	14,882	7,807	8,254	9,572	6,949	8,844	10,140	6,415	N/A	N/A	5,929	11,745	21,467	20,016	15,397	12,688	14,156	18,716
Low Volume Business Processes																							
	Authentication Select				N/A	259	142	180	160	121	169	256	125	N/A	N/A	N/A	242	275	249	204	204	240	267
	Create Request				N/A	718	620	581	780	553	1,593	1,739	1,210	N/A	N/A	N/A	1,795	3,066	2,792	2,483	2,349	2,635	3,573
	Enable/Disable Users				N/A	78	63	60	64	33,956	45	46	28	N/A	N/A	36	63	70	62	55	66	61	62
	Reissue				N/A	114	84	62	49	48	72	80	53	N/A	N/A	47	78	120	162	118	89	97	116
	Retrieve Pin				N/A	4,885	3,538	1,806	1,453	1,444	1,794	2,309	1,588	N/A	N/A	5,477	3,714	7,398	6,607	4,083	3,277	3,139	3,870
	Select Record				N/A	6,797	6,512	15,343	4,726	3,548	4,813	5,300	3,457	N/A	N/A	N/A	6,142	10,430	9,058	6,539	5,849	7,471	9,640
	Update Address				N/A	37	24	21	17	14	840	911	617	N/A	N/A	587	1,128	1,468	1,359	1,193	1,154	1,305	1,852
	Update Pin				N/A	159	84	67	66	52	78	71	48	N/A	N/A	96	87	118	117	93	86	87	100
	Check Request				N/A	1,913	5,660	14,365	1,172	921	1,251	1,445	942	N/A	N/A	N/A	1,320	2,349	2,215	1,496	1,382	1,883	2,203
Total number of transactions that the PIN database is expected to handle in an hour (at peak)	Registration					2,306	1,688	1,036	1,188	986	1,339	1,530	997	N/A	N/A	1,440	2,942	4,628	3,837	2,397	1,971	2,427	3,308
	Authentication					15,881	8,758	9,023	10,360	7,819	9,978	11,423	7,371	N/A	N/A	7,351	13,631	23,303	21,666	15,397	12,688	14,156	18,716

Note:

Existing Hits on the PIN Database come from the following applications: FAFSA 6.0, eCB, eServicing, NSLDS, STAN, and Direct Loans

Collective projections made by various client systems differed significantly from the actual results (in purple sections).

** Some of the application team could not provide the total growth - thus total growth was calculated using the standard formula.

Assumptions:

1. Some of the application team could not provide the total growth - thus total growth was calculated using the following formula. From the spreadsheet that Nina provided we have the existing hits to the pin database. We need to find the future growth (hits) to the pin database. The following formula was applied to calculate the transaction per hour.

-Traffic per month is available from Nina's spreadsheet.

For example say 1250 is the existing traffic for a month.

-Traffic growth = projected pin users - existing traffic

Traffic growth example: 1875 - 1250 = 625

-Assuming that the application is highly used 20 days a month and 15 hours each day (to get higher number of transactions) 20 days * 15 hours = 300 hours

-Transaction per hour (only growth) = Traffic growth / Number of hours

= 625 transactions / 300 hours
= 2 transactions per hour

2. FAFSA 7.0 volume is calculated by using the following formula:

This formula was derived in a meeting with Nina, NCS, and ITA.

For Authentication:

Total Existing Hits from the Pin Database * 85% (assumed distribution) * (1 + 50% (assumed growth rate))
= Projected volume

For example: February growth volume = 14882 * 85% * (1 + 50%) = 18975

For Registration:

Total Existing Hits from the Pin Database * 60% (assumed distribution) * (1 + 50% (assumed growth rate))
= Projected volume

For example: February growth volume = 2306 * 60% * (1 + 50%) = 2075