



**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

Task Order 131

ED PIN Re-Engineering Analysis

Integration Support for ED PIN Client Systems Report

Deliverable 131.1.4

Version 1.0

September 15, 2003

Amendment History

DATE	SECTION/ PAGE	DESCRIPTION	REQUESTED BY	MADE BY



Table of Contents

1	BACKGROUND	4
2	ED PIN CLIENT SYSTEMS	7
3	ED PIN RE-ENGINEERING CLIENT SYSTEM IMPACT	9
3.1	CAPABILITY ASSESSMENT	10
3.2	CLIENT IMPACT ASSESSMENT.....	11
4	SUGGESTED NEXT STEPS	13
	APPENDIX – RE-ENGINEERED ED PIN PROCESS DESIGN	15



1 Background

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 CPS¹ 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 of the credential in applications both within and outside of FSA.

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 NSLDS², access to Direct Loan Servicing website functions, access to Direct Loan Consolidation website functions, as well as for electronic signature capabilities³. 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 enterprise authentication 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 Education⁴. The following key milestones have been completed in support of this effort:

- Deliverable 131.1.2, ED PIN Updated Requirements and Standards (July 18, 2003), and
- Deliverable 131.1.3, ED PIN Technical Architecture Upgrade Analysis, Capacity Plan & Conceptual Design (August 29, 2003).

Deliverable 131.1.2, ED PIN Updated Requirements and Standards, which was completed earlier, analyzed all the current ED PIN processes, systems and associated interfaces. A high level logical overview is illustrated below. The analysis completed identified findings to address shortcomings related to process and infrastructure, data administration and evolving standards. Maintaining the integrity of the ED PIN credential data is of utmost importance

¹ Central Processing System.

² National Student Loan Data System.

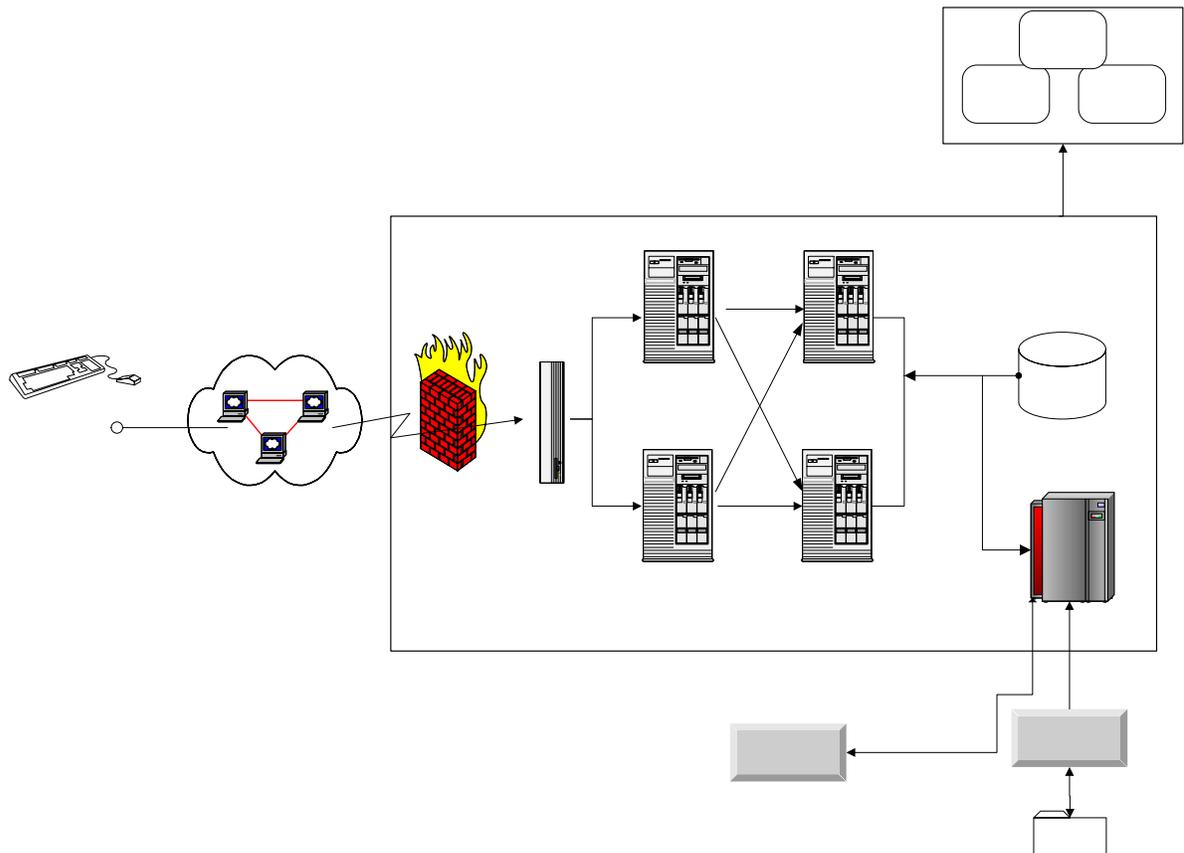
³ For example, Promissory Notes.

⁴ U.S. Department of Education Strategic Plan 2002 – 2007.



given its current and planned, expanded use for both authentication and electronic signatures. 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. The analysis recommended the following new or changed features:

- 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 a periodic refresh cycle
- Alerts and management reports
- Singular and unique user record in the ED PIN data repository
- Enhanced user self-service capabilities, and
- Standard, reusable services for identification, registration, access, self-service and administration associated with authentication.



Deliverable 131.1.3, ED PIN Technical Architecture Upgrade Analysis, Capacity Plan & Conceptual Design, elaborated on the business requirements to address technical issues related to the ED PIN re-engineering effort and capacity aspects related to the current implementation. A 4-phased approach is recommended for the ED PIN re-engineering initiative to achieve an enterprise authentication solution. The recommendations included:

- 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 capacity analysis determined that the ED PIN system does not have any critical infrastructure requirements within 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. Capacity projections will need to be re-examined upon completion of the re-engineered ED PIN system.

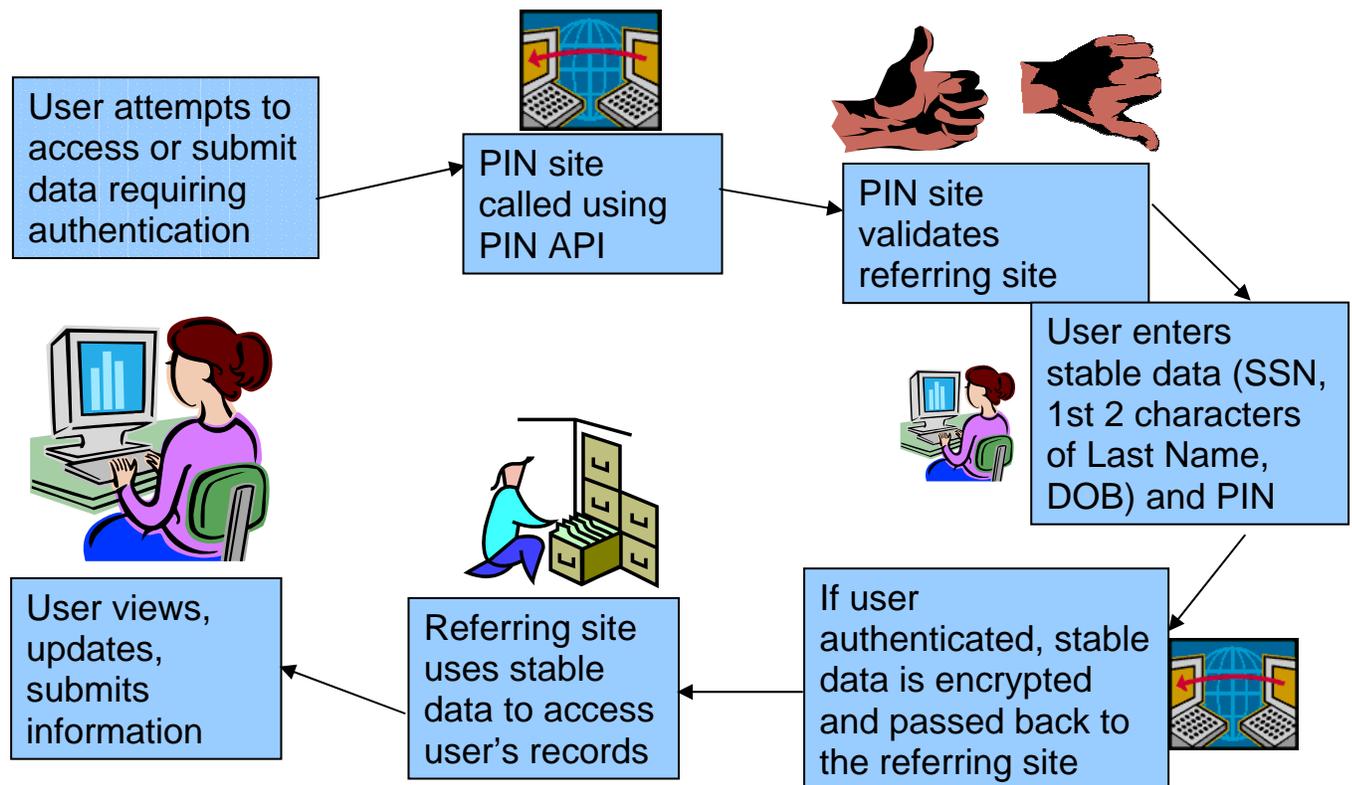
The purpose of this document is to initiate an analysis for each client system impacted from the ED PIN re-engineering effort. The impact analysis can be utilized by client systems for initial planning purposes as part of their maintenance life cycle. The client systems should validate the information within this document as part of their own assessments and the relative impact on requirements, development, testing and other appropriate phases.

2 ED PIN Client Systems

The ED PIN is the credential that is used to authenticate FSA customers. Online customer transactions with FSA systems are allowed using the ED PIN credential to authenticate users. The current FSA business systems using the ED PIN are:

- ED PIN Site
- DL Consolidation
- DL Servicing
- NSLDS
- eCB
- FAFSA on the Web
- FAA Access Online, and STAN

FSA PIN Authentication Process



The ED PIN will be the enterprise tool for the authentication of borrowers online and not trading partners (schools and financial partners). This will exclude FAA's, and eCB, who would eventually transition towards another method of authentication for their users.

This initiative envisions the ED PIN as an Enterprise Authentication Service for students, parents and borrowers. As appropriate, FSA may want to transition other FSA systems to consolidate and use the ED PIN credential for authentication. The ED PIN should be a flexible and viable enterprise resource to accept other efforts which may require systems outside FSA to use the ED PIN credential for authentication. Future uses of the ED PIN credential in consideration may include the Student Portal, authenticating E-Servicing IVR, Common Services for Borrowers (CSB) and E-Gov initiatives.

3 ED PIN Re-Engineering Client System Impact

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 possesses 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 users or systems) while

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

simultaneously strengthening the integrity of the ED PIN credential. The re-engineered ED PIN is designed to 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. The Enrollment and Access Management initiative will determine the

appropriate credential for trading partners. Upon selection of an appropriate solution, a plan to transition FAAs to a different authentication credential will be developed as part of the Identity and Access Management (I&AM) initiative. The registration process continues 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 will be formalized as an annual activity to ensure all requirements are known and tested. Functionality within the registration process distinguishes 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 capability separates 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. The re-engineered PIN enhances Self-service functionality to encourage increased use of the ED PIN while minimizing help desk contact. And finally, the administration process is 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.



3.1 Capability Assessment

The following table describes capabilities and impacts of the re-engineered ED PIN system by high level business function.

Functionality	Current Capability	Client System Impact	User Impact	Benefit
Identification	System - No (Informal) User - Yes	<ul style="list-style-type: none"> • Need to possess Digital Certificate 	None	<ul style="list-style-type: none"> - Validity of Authentication Requests - Communication
Registration	System - No (Incomplete) Client - Yes	<ul style="list-style-type: none"> • System Registration Process • Test re-Engineered ED PIN • Select Access Protocol • Transition FAA's from ED PIN • Client Registration Function <ul style="list-style-type: none"> - SSA Verification - Non-SSA Verification Credential (Optional) 	<ul style="list-style-type: none"> • Authentication Functions for Pseudo-SSN • Single ED PIN 	<ul style="list-style-type: none"> - No Duplicate ED PIN Records - Transaction Logging - Management Reports - Standard Interface - SSA Computer Matching
Access	System - Yes User - Yes (No distinction between Authentication & e-Signature)	<ul style="list-style-type: none"> • Upgrade Access Protocol for Authentication and e-Signatures 	None	<ul style="list-style-type: none"> - Authentication (including pseudo-SSN) - e-Signature compliance (SSA Match Only)
Self-Service	System - No User - Yes	<ul style="list-style-type: none"> • SSIM Implementation 	None (Authentication Required for Self-Service)	<ul style="list-style-type: none"> - Enhanced Functionality
Administration & Management	System - No (Incomplete) Client - N/A	<ul style="list-style-type: none"> • Option for Additional 3rd party verification (for ED PIN Only) 	None	<ul style="list-style-type: none"> - Reporting - Communication (Including Alerts)

3.2 Client System Impact Assessment

The following table lists the high level impact to Client Systems based on ED PIN Re-engineered capabilities. General Client System Impacts apply to the following FSA client systems: FAFSA on the Web, Direct Loan Servicing, Direct Loan Consolidations, and National Student Loan Data System (NSLDS). Note: Direct Loan Servicing will be specifically impacted in the process of directly creating ED PIN accounts for unmatched records in the demographic update process. Unmatched records will be batched to undergo the Client Registration Process which is subject to an SSA match. Impacts to technical architecture, capacity, and performance need to be re-visited based on the outcomes of the Tools Analysis initiative. Direct Loan Servicing and Direct Loan Consolidation will incorporate the re-engineered ED PIN into the CSB initiative.

FSA System	Need to possess Digital Certificate	System Registration Process	Test Re-engineered ED PIN	Select Access Protocol	Transition FAA's from ED PIN	Client Registration Function SSA Verification Non-SSA Verification Credential (Optional)	Upgrade Access Protocol for Authentication and e-Signatures	SSIM Implementation	Option for Additional 3rd party verification (for ED PIN Only)	Authentication Functions for Pseudo-SSN	Single ED PIN
ED PIN	The ED PIN functions will be part of an ED PIN system possessing it's own unique credential such as a digital certificate	ED PIN system will require a formal application process for client systems. The process will include a formal application about client system usage (authentication, e-signature) and volume of usage (capacity plan) for ED PIN transactions. -Add functionality to authenticate registered client systems.	- ED PIN system will create testing protocol for transition of client systems.	- Establish a standard suite of access protocols for interfacing with the ED PIN system. - Client systems will select preferred protocol from this suite.	Re-engineered ED PIN system will not accept any new FAA credentials and a plan must be devised to transition existing FAA's to new credential. The ED PIN system will participate in the development of FSA Enrollment and Access Management standards.	- All client systems requesting the creation of an ED PIN record must undergo the Client Registration process; which includes a SSA match. - For non-standard SSNs (pseudo SSNs issued by client systems), client systems will have the option of requesting an ED PIN on behalf of the user (not subject to SSA match). These users will have the ability to authenticate to client systems with an ED PIN. However, these users will not have e-signature capability with their ED PIN.	- ED PIN system will upgrade specifications for authentication and e-sign functionality. - ED PIN will develop a transition plan to migrate Client systems to the new access protocols. - STAN functions will be serviced through ED PIN system	Recommended in requirements for re-engineered ED PIN.	- ED PIN system design includes additional verification (e.g., Homeland Security) before an ED PIN record is generated. This check may also apply to pseudo SSNs. - the design is flexible to incorporate additional checks at any stage of the ED PIN record (e.g., prior to or subsequent to issuance of an ED PIN)	Will need to develop pseudo SSN authentication business logic.	Multiple PINs will not be supported for a single SSN record.



FSA System	Need to possess Digital Certificate	System Registration Process	Test Re-engineered ED PIN	Select Access Protocol	Transition FAA's from ED PIN	Client Registration Function SSA Verification Non-SSA Verification Credential (Optional)	Upgrade Access Protocol for Authentication and e-Signatures	SSIM Implementation	Option for Additional 3rd party verification (for ED PIN Only)	Authentication Functions for Pseudo-SSN	Single ED PIN
General Client System Impacts	All systems will need to adapt their interface protocols to allow for a credential such as a digital certificate.	Systems will be required to complete the formal application about their usage (authentication, e-signature) and volume of usage (capacity plan) for the ED PIN system. -All client systems must add functionality to identify themselves to the ED PIN (i.e., digital certificate)	- Systems will need to test functionality and connectivity to the re-engineered ED PIN. - Systems will be required to successfully test interface to ED PIN on an annual basis as part of the System Registration Process	All client systems adhere to access protocol standards established for interfacing with the ED PIN system.	None	Client systems will need to modify their processes to adhere to the Client Registration batch protocol. This includes an ability to flag pseudo SSN records if they wish to give these users electronic access to their system. (Creation of ED PINs from unmatched records on client system batch files for the purpose of demographic updates will no longer be allowed.)	All systems will need to modify their current interface (and possibly business process) to comply with new standards to account for authentication and e-signature functionality enhancement.	ED PIN will interface with SSIM enabled systems for demographic updates ⁵ .	None	Client systems will have the option to allow pseudo-SSN users electronic access to their systems. Systems desiring this functionality may be required to modify their systems to pass pseudo-SSN information. Note: e-signature capability will not be offered to pseudo SSN users.	Users that access the FSA applications with an older ED PIN will need to have the current ED PIN sent to them.
eCampus Based	Transition to trading partner credential, as to be recommended by Enrollment and Access Management initiative.										
FAA Access Online											

Client Systems are advised to use this report as input towards their own impact analysis for the re-engineered ED PIN. More detailed information regarding Client System impacts will be elicited as the re-engineering process continues. The upcoming events related to the realization of the re-engineered ED PIN vision is detailed in the following section.

⁵ Client System impacts will be determined upon completion of activities by the Data Strategy Enterprise initiative.



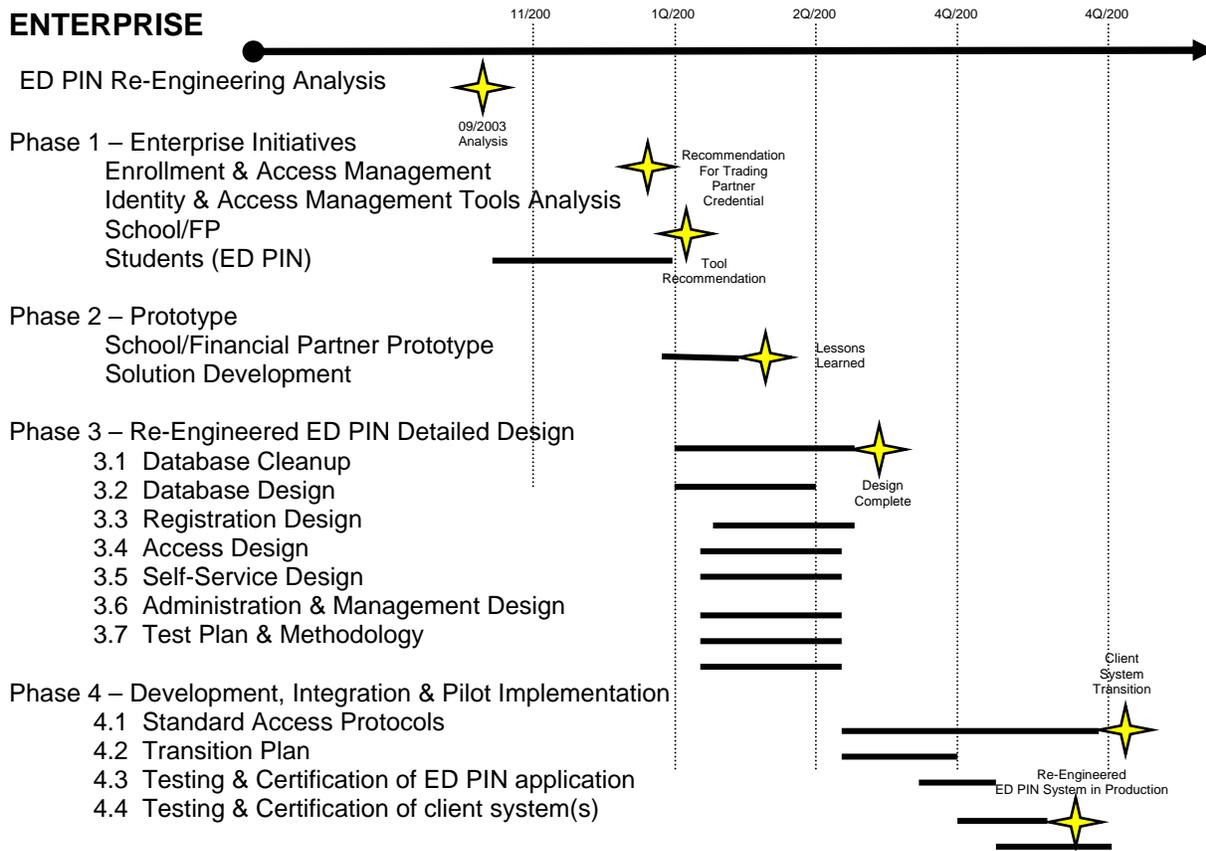
4 Suggested Next Steps

This deliverable completes the enterprise authentication vision effort associated with the ED PIN re-engineering effort. Next steps are suggested in this section for FSA to implement the enterprise authentication vision based on milestones completed earlier. The milestones completed include the requirements and standards, technical architecture and conceptual design.

A 4-phase approach is recommended to mitigate operational risks. Phase 1, Enterprise Initiatives, will result in (a) recommendations for an appropriate credential for trading partners that currently use the ED PIN (Enterprise Initiative – Enrollment & Access Management - EAM) and (b) recommendations for commercial-off-the-shelf (COTS) tools for identity and access management functionality (Enterprise Initiative – Identity & Access Management - I&AM). The names, schedule and deliverables of these 2 enterprise initiatives are presented as currently known.

Coordinating the ED PIN re-engineering efforts in Phase 1 with other relevant enterprise initiatives is important for two reasons. First, recommendations for the credential(s) to be used by trading partners – especially for Financial Aid Administrators (FAAs) is relevant to the ED PIN re-engineering effort. FAAs currently use their ED PIN credential for authentication to the E-Campus based and FAA Access Online applications. If the initiative recommends a credential different from the ED PIN for FAAs then the ED PIN re-engineering effort will need to participate in a transition plan for them. If the initiative recommends continued use of the ED PIN for FAAs, then the ED PIN re-engineering effort will need to accommodate them as part of its requirements and design. Second, COTS recommendations from the I&AM effort underway will impact the detailed design for the re-engineered ED PIN system.

Phase 2, Prototype, is another Enterprise Initiative, which will result in understanding the COTS recommendations through a limited, physical implementation. The ED PIN re-engineering effort can benefit from any lessons learned as a result of the prototype to update requirements, standards, technical architecture and/or conceptual design, as appropriate. This phase is an important stage of the ED PIN re-engineering effort due to the anticipated COTS recommendations from Phase 1. Participation in the prototype will yield important pragmatic considerations that can be incorporated into the design during Phase 3.



Phase 3, Detailed Design, can leverage the results from the earlier phases to design the re-engineered ED PIN solution. The objective of Phase 3 is to perform detailed planning and design activities for the ED PIN re-engineering effort. Activities illustrated (e.g., database related, process related, and planning related) are only representative and will need to be appropriately planned.

Phase 4, Development, Integration & Implementation, refers to the deployment of the re-engineered ED PIN solution. The objective of this is to develop and deploy the ED PIN re-engineering solution. Client systems should be transitioned to the re-engineered solution upon certification and accreditation of the re-engineered ED PIN solution.

The phased approach will help FSA take advantage of other related and ongoing enterprise initiatives and help mitigate risks by instituting appropriate project milestones and management reviews.



APPENDIX - RE-ENGINEERED ED PIN PROCESS DESIGN

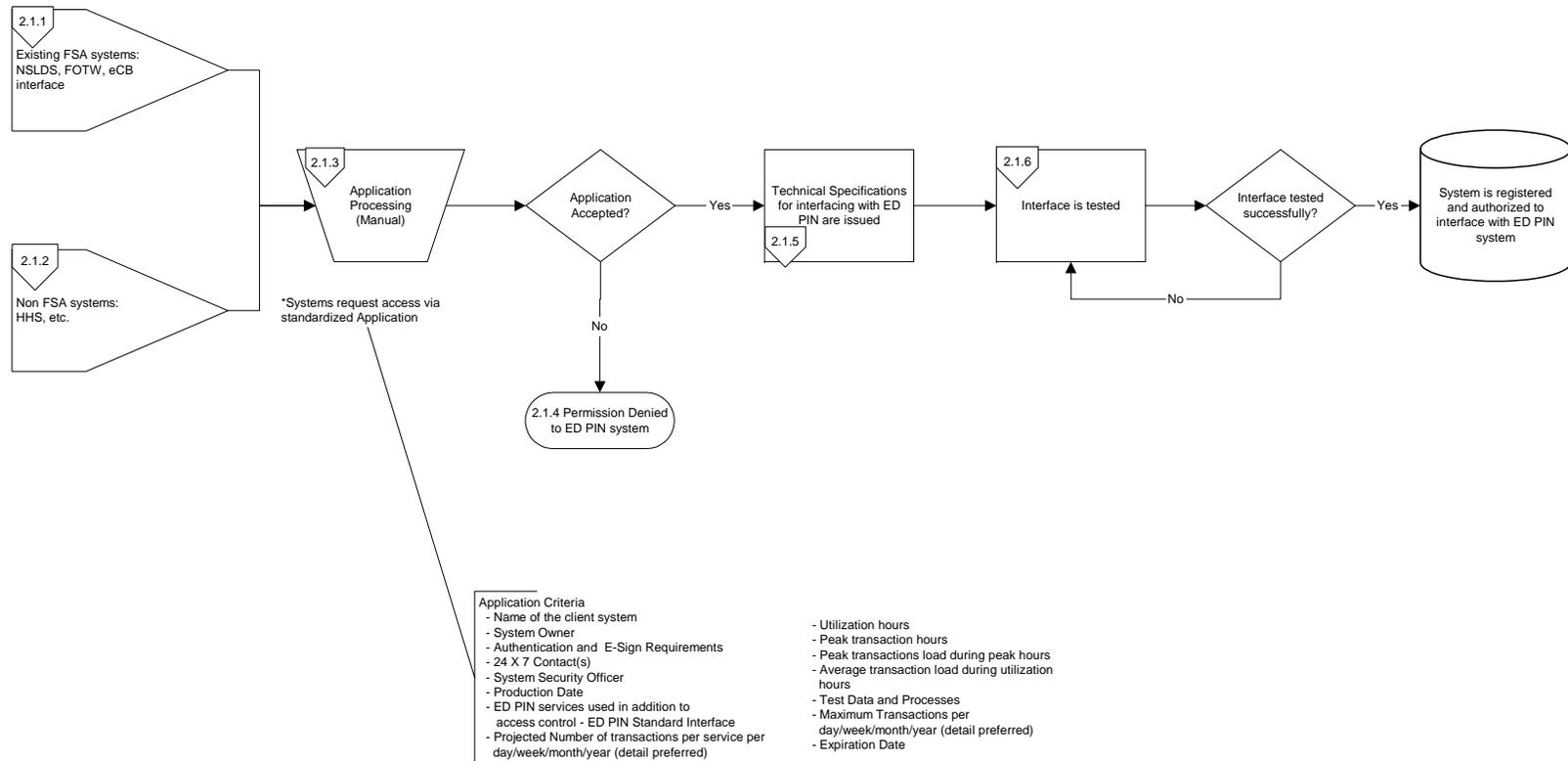
Referenced from Deliverable 131.1.3 ED PIN Technical Architecture Upgrade Analysis,
Capacity Plan & Conceptual Design (August 29, 2003)

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

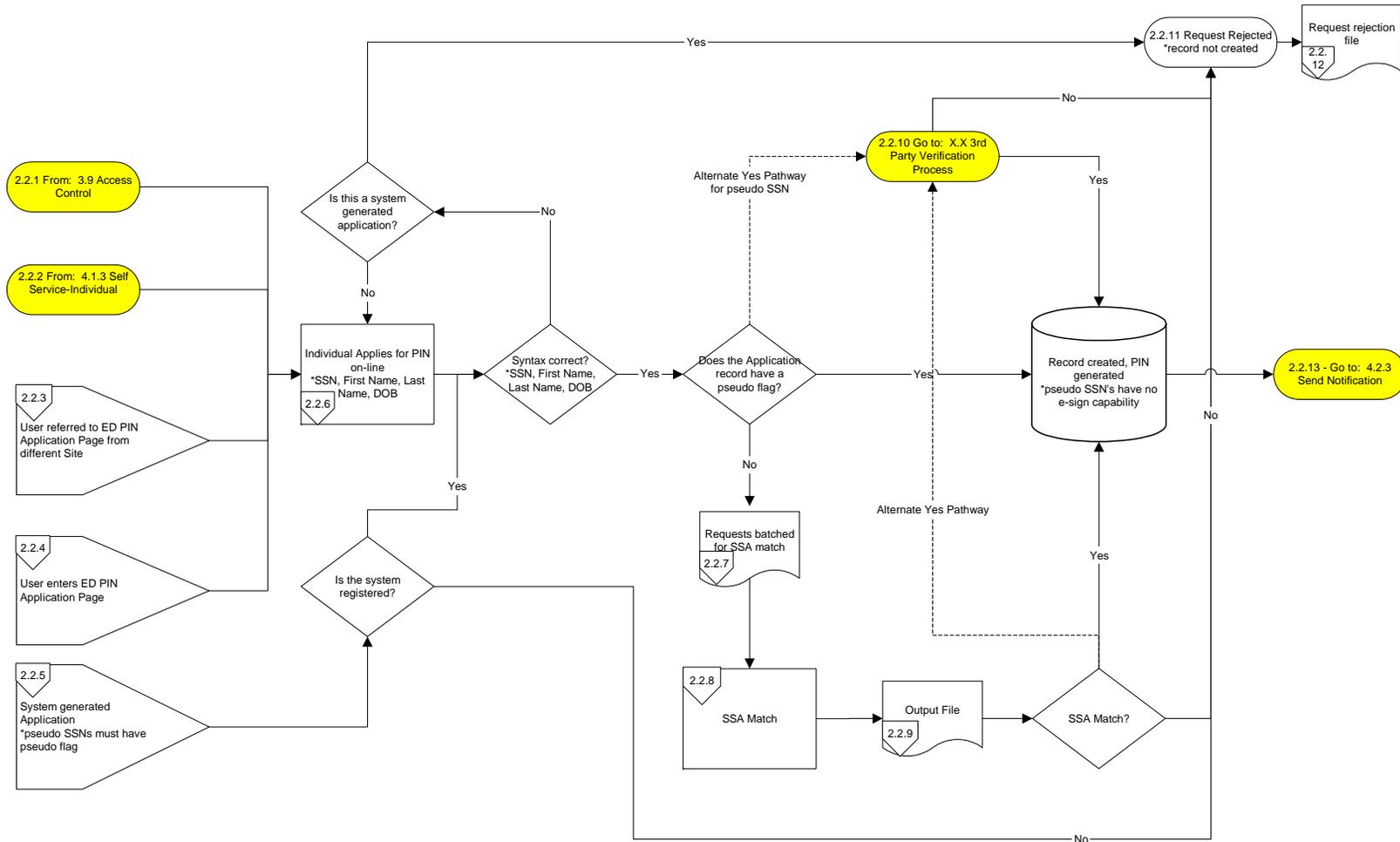


ED PIN Re-engineering Process Design

Process: Registration (Individual)

Process ID: 2.2

Description: The process of applying for ED PIN

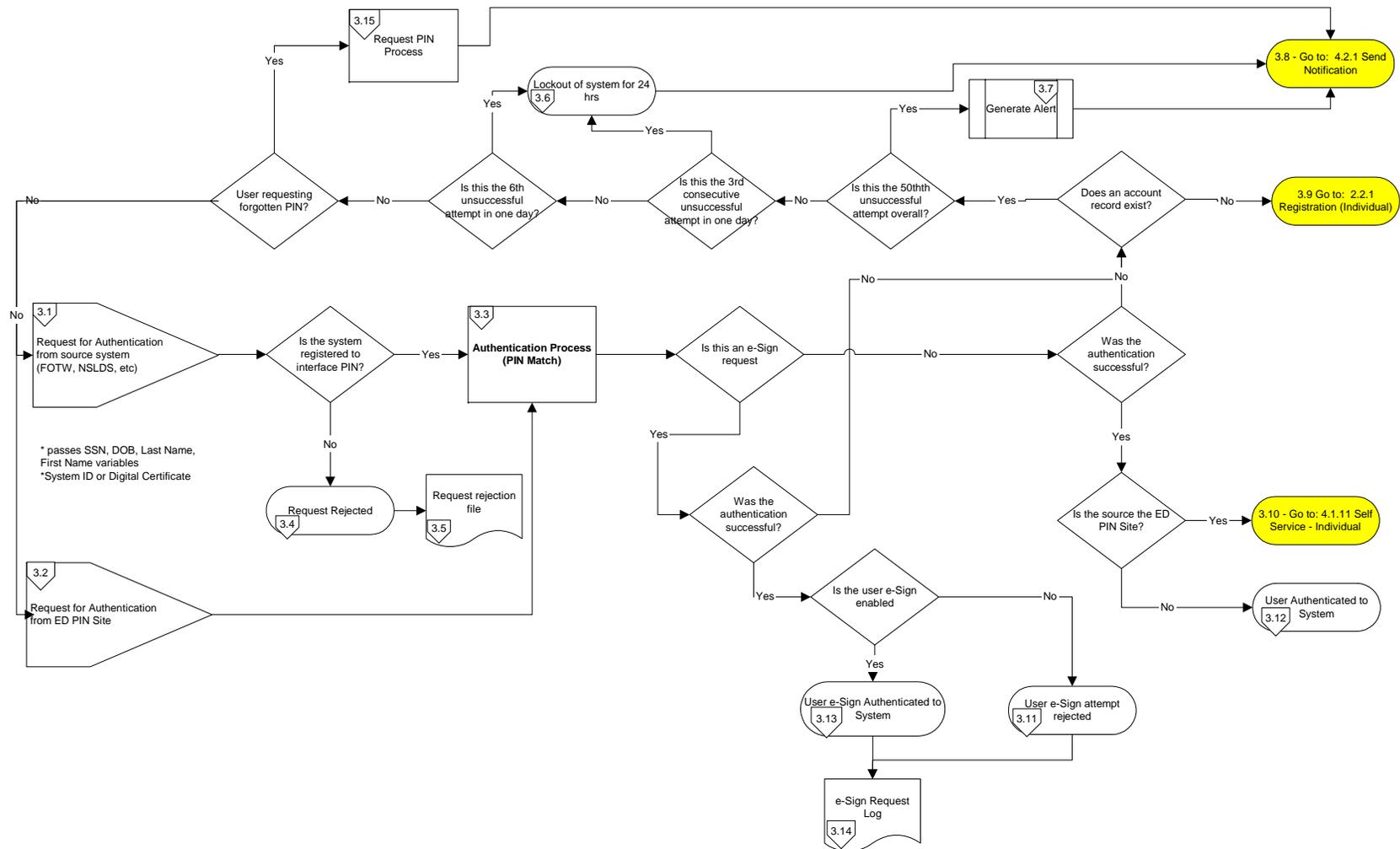


ED PIN Re-engineering Process Design

Process: Access Control

Process ID: 3.0

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

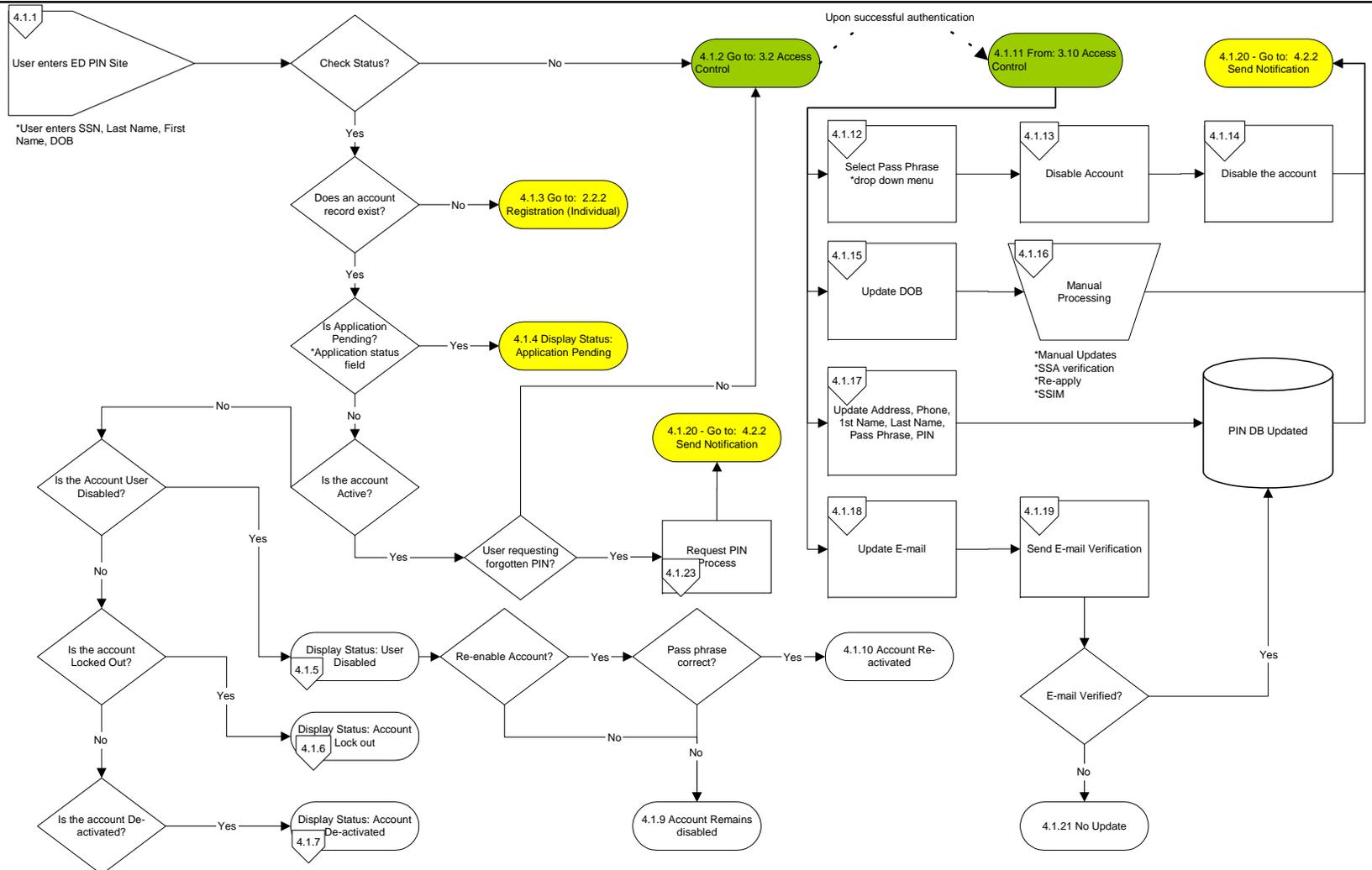


ED PIN Re-engineering Process Design

Process: Self Service - Individual

Process ID: 4.1

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

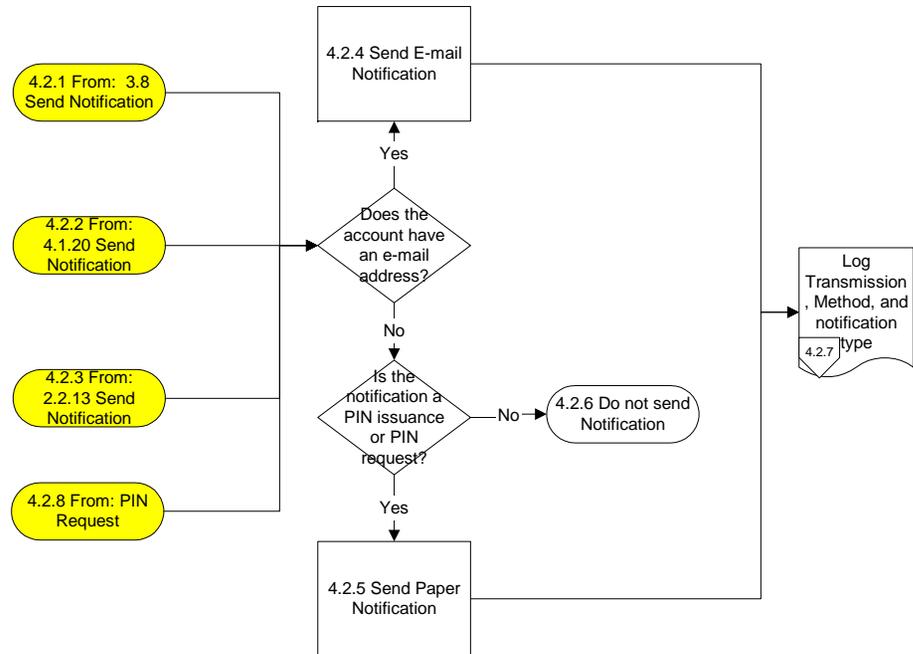


ED PIN Re-engineering Process Design

Process: Self Service (Notification Process)

Process ID: 4.2

Description: The process of Sending Notification to Users



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

