



**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 144

E-Authentication & E-Signature Support

# E-Authentication Opportunities Support Performance Report – January 2004

**Deliverable 144.2.1**

**January 31, 2004**

## TABLE OF CONTENTS

<b>AMENDMENT HISTORY .....</b>	<b>2</b>
<b>1 INTRODUCTION &amp; ORGANIZATION OF THE DOCUMENT.....</b>	<b>3</b>
1.1 INTRODUCTION.....	3
1.2 ORGANIZATION OF THE DOCUMENT .....	3
<b>2 COMMENTS ON EXTERNAL RELATED DOCUMENTATION.....</b>	<b>4</b>
<b>3 WHITE PAPER: E-ID TRUST FOR FSA EXTERNAL OPERATIONS.....</b>	<b>5</b>
<b>4 ED PIN SUPPORT ACTIVITIES.....</b>	<b>8</b>
<b>5 E-AUTHENTICATION PILOT SUPPORT ACTIVITIES.....</b>	<b>9</b>
5.1 FSA – HHS E-AUTHENTICATION PILOT .....	9
5.2 ED PIN COMPUTER MATCHING AGREEMENT (CMA) ACTIVITIES .....	9
5.3 EDUCAUSE – NIH PILOT .....	11
<b>6 REFERENCES .....</b>	<b>12</b>
6.1 PROJECT WORK PLAN.....	12
6.2 PROJECT MEETINGS.....	14
6.3 WHITE PAPER: DEVELOP AN FSA E-AUTHENTICATION, E-ID & E-SIGN BUSINESS PLAN.....	19
6.4 COMPUTER MATCHING AGREEMENT (CMA) PROCESS DOCUMENTATION .....	27

## Amendment History

DATE	SECTION/ PAGE	DESCRIPTION	REQUESTED BY	MADE BY

## 1 INTRODUCTION & ORGANIZATION OF THE DOCUMENT

### *1.1 Introduction*

The FSA Integration Partner is one of multiple groups working with the Office of Applications Development in its implementation of E-Gov E-Authentication initiatives; both internally within FSA as well as externally across agencies. During January, 2004, the initiatives supported include the inter-agency computer matching agreement activities, the ED PIN credential assessment activities, updates to the previous deliverable (Deliverable 144.1.1), review of documents, initial identification of candidate forms for the EDUCAUSE-NIH PKI pilot and continued development of the White Paper for E-ID / E-Authentication / E-Sign.

The purpose of this performance report is to document the FSA Integration Partner activities during the month of January, 2004. This report details activities during this current reporting period. A White Paper documenting FSA's E-ID, E-Authentication and E-Sign direction is also included as part of this deliverable. This White Paper is an extension to a previous version that focused on internal activities; this version focuses on external positions; both, versions seek to further strengthen FSA capability.

### *1.2 Organization of the Document*

The following sections within this document include:

- Comments on external, related, documentation
- Updated White Paper on E-Authentication for FSA external operations
- Activities supported for the ED PIN
- Activities supported for the E-Gov E-Authentication pilot

Project meeting related information, including a current project work plan, and a previous White Paper are included in the References section at the end of the document.

## 2 COMMENTS ON EXTERNAL RELATED DOCUMENTATION

During January, 2004, the following document was reviewed at FSA request. The document is external to FSA but related to ongoing project activities: Information Security: Status of Federal Public Key Infrastructure Activities at Major Federal Departments and Agencies. GAO-04-157, December 15. The review provided to the FSA project manager is noted following the next paragraph.

During this period, Integration Partner also received the following documents related to the ED PIN credential assessment: Checklist for Password Credential Assessment – Interim v0-1-5i, Credential Service Provider Application, E-Authentication Interim Common Credential Assessment Profile release 1.3.0, E-Authentication Interim Credential Assessment Guidance release 1.3.0, E-Authentication Interim Credential Assessment Framework release 1.3.0, E-Authentication Interim PKI Credential Assessment Profile release 1.3.0, and E-Authentication Interim PIN Credential Assessment Profile release 1.3.0. These documents were not reviewed during this period.

**Review GAO PKI Report** – comments on “Information Security: Status of Federal Public Key Infrastructure Activities at Major Federal Departments and Agencies. GAO-04-157, December 15 <http://www.gao.gov/cgi-bin/getrpt?GAO-04-157> Highlights - <http://www.gao.gov/highlights/d04157high.pdf>”. The report is an excellent compilation of PKI initiatives within the Federal environment, the challenges as well as the strength of the technology. It highlights the 4 challenges as being policy and guidance, funding, interoperability, and training and administration. The reports acknowledges the strength of PKI technology over password-based systems – it does not, however, acknowledge any limitations of the technology itself. From FSA’s business perspective, the report lacks a discussion on alternative solutions where PKI is not an option for identification, authentication or electronic signature (e.g., business transactions with public citizens). The report also lacked a discussion of industry efforts where basic PKI capabilities are enabled as part of the desktop operating system and the future implications thereof. The report does provide a good discussion from the technical and policy perspective but lacks a discussion on business use. This is, perhaps, where GAO’s recommendation for a framework from OMB may fill the void. The conclusion states the framework will help with “consolidation of PKI technology across Government”; focus would be better served if the objective included interoperability standards between Government and private sector. Washington Technology ([http://www.washingtontechnology.com/news/1\\_1/daily\\_news/22526-1.html](http://www.washingtontechnology.com/news/1_1/daily_news/22526-1.html)), Government Computer News ([http://www.gcn.com/vol1\\_no1/daily-updates/24644-1.html](http://www.gcn.com/vol1_no1/daily-updates/24644-1.html)), and many other publications also reported the GAO findings.

### 3 WHITE PAPER: E-ID TRUST FOR FSA EXTERNAL OPERATIONS

Waves of information technology innovations, especially during the past few decades, have given organizations an unprecedented ability to get to know their customers. Indeed, technologies such as the Internet, portals, wireless communications, Web services, and in-vehicle telematics will likely enable the collection of richer, more robust, and often more personal, data on their customers than ever before. Using the latest analytical tools, forward-thinking companies are mining that data for important insights that can help them provide more tailored, personalized customer service, wherever their customers are. The fact remains, that to profit from customer relationships organizations must build and maintain lasting relationships first. In an era where traditional interaction (e.g., face-to-face) is diminishing while the frequency of interaction is increasing, the mere recognition of a customer – consistently accurate, regardless of communication medium – is becoming the cornerstone to providing commodity products and business services. FSA’s approach to electronic identities (E-ID) and related business services (e.g., E-Authentication and E-Signature today, and Single Sign-On in the future) needs to be based on ensuring and building trust.

The ED PIN continues to be the FSA E-ID for its student and parent customers. It facilitates e-authentication as well as e-signature. Furthermore, the same services are proliferating even outside the FSA organization – for student and parent transactions with Schools (e.g., Perkins promissory notes) and other Federal agencies (e.g., DHHS). The ED PIN is continuing to build upon its established trust through both the ED PIN re-engineering initiative as well as external assessment of its strength. The re-engineering initiative establishes the ED PIN as an enterprise service for customers seeking to do business electronically with FSA. The external assessment planned with NIST-based guidelines through GSA further establishes FSA’s commitment to earning customer trust.



*FSA’s E-ID product and business services continue to build customer Trust.*

This White Paper proposes 5 elements of Trust as governing principles for FSA's E-ID efforts. These elements include:

1. **Security**. Customers are confident that their personal information is protected against theft or other unauthorized use; whether in storage (e.g., database) or during communication (e.g., SSL encryption).
2. **Data Control**. Customers have control over who gains legal access to their information as well as when they get access and what they can do with it. This element will need to be further pronounced as FSA extends relationships with other business partners using the same electronic credential.
3. **Personal Access**. Customers control who reaches them and through which medium. Not all transactions are "personal" in nature - as such, there is a need to distinguish between identification of personal versus organizational entity.
4. **Benefit**. Customers are assured that the organization is not using their data simply for business advantage, but is offering them reciprocal benefits that are directly relevant and known to customers.
5. **Accountability**. When they grant access to their information, customers know that this access will be used responsibly and in their best interests. If not, someone will take the responsibility for the misuse and take corrective action.

These elements will apply regardless of how FSA identifies electronic customers (i.e., through the use of an ED PIN, transitive trust protocols, or PKI) and regardless of communication medium (i.e., in-person, via a web portal, subscription to web services, through a mobile platform or even a different affiliation such as a School). As long as FSA's E-ID product and service provides uncompromising trust, both the customer and FSA will continue to reap efficiencies.

Making the FSA E-ID the credential of choice (e.g., among students) will require a formal process for building and sustaining trust. This process can be inherent within the FSA E-ID enterprise governance process. The formal process can initially benefit from 6 specific activities:

#### **A. Plan Your Trusted Services**

Trust doesn't simply continue to happen. As part of the overall business plan, decide what sorts of new services will be planned, piloted, developed, and deployed - and know what will be required to create the appropriate environment of trust to ensure the success of those services.

#### **B. Understand Trust in Your Customer Base**

Every business is different, so it's important to clarify the unique concerns and motivations of the customer base when it comes to privacy and trust. Customer needs may differ on the basis of product (e.g., stage in life cycle) or service (e.g., identification, authentication, electronic signature, etc.). For example, it may be necessary to pioneer innovative solutions that issue unique, one-time-use-only credentials for certain types of transactions.

### **C. Make Your Trust Policy and Approach Clear**

Develop and publish a set of guidelines about how customers' personal information and privacy is protected. It may help to conduct an internal audit of these guidelines and enforce them both internally and with appropriate business partners. One parallel here is the Graham-Leach-Bliley Act, which informs individuals about the privacy policies and practices of financial institutions so that consumers can use that information to choose the companies with which to do business. Trustworthiness is likely to be a similar kind of basis of consumer choice. It's not a stretch to say that trust may join other intangibles such as brand perception and shopping experience on the "balanced scorecard" that customers use to select their preferred providers.

### **D. Become Part of a Trusted Value Chain**

Work with your business partners so that all partners are simultaneously collaborating to provide the same degree of trust and responsibility across the value chain. In fact, one goal to work toward may be to create a hierarchy of trust. However, any organization that vouches for the security and reputation of a trading partner had better be sure of that reputation and know what that partner will do with customer data.

### **E. Be Trustworthy Within Your Organization as Well**

To establish trustworthiness externally, it will first need to be established internally. Some successful techniques have included educational campaigns to reinforce key values and ethical tenets, posting code of conduct and expectations for employee/contractor behavior, or even sponsor awards that recognize the exhibition of the highest standards.

### **F. Influence Relevant Governing Bodies**

Actively monitor legislative and regulatory developments and demonstrate to the appropriate governing bodies and customer associations (e.g., EDUCAUSE) that as you design and implement new services, you also are taking active steps to promote trustworthy and responsible use of consumer data.

Because the proliferation of technologies and the fear of abuses such as identity theft have heightened legitimate concerns about the privacy of individuals and their data, many organizations today are reluctant to use information in ways that could better serve their customers and create new products and services. Yet, in being too cautious, these organizations put themselves at a disadvantage. Instead, FSA is promoting the expanded use of its credential. The risks are the same either way and require mitigation.

Customer adoption of the electronic identities and related services is continuing to grow. The responsibility for mitigating potential risks needs to be visibly and formally executed.

**NOTE:** This White Paper is an addendum to an earlier Deliverable 144.1.1. The previous White Paper is attached in the References section.

## 4 ED PIN SUPPORT ACTIVITIES

During this period, FSA completed all planning activities for the formal ED PIN credential assessment. A high level activity plan was provided by Integration Partner to the FSA project manager and included the following tasks:

1. Receive current CAF including PIN CAF and NIST 800-63.
2. Formulate FSA Executive Team for Credential Assessment.
3. Establish FSA Support Team for Assessment (resource allocation).
4. Schedule ED PIN credential assessment date(s).
5. Seek lessons learned and best practices from assessment completed/underway by GSA.
6. Collect/compile/update documentation, as necessary.
7. Submit questions to GSA assessment team.
8. Kick-off meeting for ED PIN credential assessment.
9. ED PIN credential assessment (2 days).
10. ED PIN credential assessment debrief.
11. ED PIN credential assessment debrief – executive team.
12. Determine Next Steps.

Tasks 1 – 4 have been completed by FSA, tasks 5 – 7 are in progress by FSA, and the formal assessment (tasks 8 – 12) has been planned; with the kick-off meeting (task 8) scheduled for February 6, 2004. It is anticipated that the ED PIN credential assessment will be complete by February 13, 2004.

## 5 E-AUTHENTICATION PILOT SUPPORT ACTIVITIES

### 5.1 FSA - HHS E-Authentication Pilot

The E-Authentication pilot with HHS remains on hold pending final E-Authentication Architecture guidance from the E-Gov team. As such there were no support activities during this period directly with HHS. However, FSA continued to work with SSA to execute a revised computer matching agreement for expanded use including the FSA HHS pilot. Current status related to the computer matching agreement is documented in the following sub section.

### 5.2 ED PIN Computer Matching Agreement (CMA) Activities

Integration Partner worked with FSA to understand the activities required for the revised computer matching agreement (CMA). The 18 month process as documented by Marya Dennis (FSA) is attached in the reference section of this document (section 6.3). Ms. Dennis prepared a work plan for the FSA CMA that is referenced in the e-mail below. Activities are tracking to plan.

**From:** Dennis, Marya [Marya.Dennis@ed.gov]

**Sent:** Friday, January 23, 2004 3:30 PM

**To:** Katyal, Yateesh

**Cc:** Sattler, Neil

**Subject:** RE: CMA Approval Process Documentation Walkthrough

Neil and Yateesh:

It was nice meeting you this afternoon. This is the framework I understood from our conversation. I've taken the liberty of adding details to determine the entire time line. There may be some places where we can save time. It will depend on communications and luck. Please let me know if you have revisions or questions or concerns.

**By Jan. 30:**

- Ronn Sann will send me a draft of the Amendment.

**By Feb. 2:**

- MD will distribute the Amendment to Kelly Elsworth at SSA for an informal review. (cc: Bill Leith & Dan Klock).

- MD will ask Kelly for an estimated deadline for a revised draft from SSA (hopefully 2 wks).

- Ronn Sanns and Kelly can meet to resolve issues. Or, I'll coordinate meetings if necessary.

**By Feb. 17:**

- MD will receive a revised final from SSA.

- MD will send a copy to Sanns, Sattler, Coleman, Katy, Leith and Klock.

- MD will email a copy of the amendment to Leslie Sommerville in DRM for Federal Register review and clearance. Sommerville will send DRM Attorney comments to MD over the next 3 weeks. MD will make minor changes and coordinate any significant changes with Sanns.

**By Feb. 24:**

- MD will create a correspondence summary and send the amendment up the FSA chain for signatures. This usually takes 1 to 2 weeks. DRM changes can continue during this process.

- MD will ask Alexia Roberts to prepare letters to notify Congress and OMB of the amendment.

**By March 9:**

- The Amendment should be signed by Terri Shaw.
- MD will send the Amendment to SSA for clearance. Kelly will have to give us a time frame. I'm guessing 3 weeks. [As soon as SSA tells me it is ok and will be signed, I can start getting FSA signatures on the Fed Register notice].

**By March 30:**

- Kelly will send me a signed copy of the Amendment.
- MD will send the final Federal Register notice through FSA signature clearance (1 to 2 weeks).

**By April 13:**

- MD will hand carry the final copy of Federal Register Notice (with signatures) to Somerville for publication. This usually takes 5 days to publish.
- MD will notify Alexia to sign, date and transmit letters to Congress and OMB.

**April 19:**

Fed Register Notice is printed

**May 29**

40 days after Fed Register publication, we can begin pilot.

-----Original Message-----

**From:** yateesh.katyal@accenture.com [mailto:yateesh.katyal@accenture.com]

**Sent:** Friday, January 16, 2004 2:20 PM

**To:** Dennis, Marya

**Cc:** Sattler, Neil

**Subject:** CMA Approval Process Documentation Walkthrough

Marya:

Thank you very much for your help in understanding the review and approval process associated with the computer matching agreement. As I mentioned during our phone conversation, I am working for Mr. Neil Sattler in the CIO's office which has responsibility for overseeing the approval of the updated CMA.

I will look forward to receiving the process documentation from you and our meeting next Friday (January 23, 2004) at 1:30pm.

Please feel free to contact me via e-mail ([Yateesh.Katyal@Accenture.com](mailto:Yateesh.Katyal@Accenture.com)) or telephone in case you have any questions.

Best Regards,

Yateesh Katyal, Ph.D.  
202-962-0882 (office)  
410-908-5371 (cell)

This message is for the designated recipient only and may contain privileged, proprietary, or otherwise private information. If you have received it in error, please notify the sender immediately and delete the original. Any other use of the email by you is prohibited.

### 5.3 EDUCAUSE - NIH Pilot

For the EDUCAUSE-NIH PKI pilot, Integration Partner and FSA have identified potential form candidates for consideration. The potential form candidates are noted below. FSA is not a current participant in the EDUCAUSE-NIH PKI pilot. The potential form candidates have been identified in case FSA decides to participate in the pilot. One reason FSA could benefit from participation is to learn first-hand about the business applicability of PKI technology to FSA business processes. Another reason FSA could benefit from participation is to demonstrate continued partnership with EDUCAUSE and School (FSA customers) participants. A third reason for FSA to participate is that the initial pilot investment - fixed cost - for hardware, software, processes, resources, etc. has already been incurred. The cost for FSA participation will only be incremental and minimal. Participating schools in the EDUCAUSE - NIH PKI pilot include - University of California (Berkeley), University of Texas - Health Sciences Center, Dartmouth College, University of Virginia, University of Wisconsin (Madison) and University of Alabama.

Potential form candidates for consideration, if FSA participates in the pilot are:

- A. ED 424 Form - Application Form for Federal Education Assistance
- B. ED 524 Form - Budget Information, Non-Construction Programs
- C. ED 524-B Form - Grant Performance Report
- D. ED 80-0013 Form - Certifications Regarding Lobbying; Debarment, Suspension and Other Responsibility Matters; and Drug-Free Workspace Requirements
- E. ED 80-0014 Form - Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion - Lower Tier Covered Transactions
- F. ED 80-0016 Form - Certification of Eligibility for Federal Assistance in Certain Programs
- G. SF 424B Form - Assurances, Non-Construction Programs
- H. SF LLL Form - Disclosure of Lobbying Activities
- I. SAIG Enrollment Document
- J. Equity in Athletics Disclosure Act
- K. Fiscal Operations Report and Application to Participate in Opportunity Grant, and Federal Work-Study Programs
- L. Student Assistance General Provisions - Subpart K - Cash Management
- M. Federal Pell Grant Program Recipient Financial Management Systems (RFMS)
- N. Application for Approval to Participate in Federal Student Financial Aid Programs
- O. Fiscal Operations Report and Application to Participate (FISAP) in the Federal Perkins Loan, federal Supplemental Educational Opportunity Grant, and Federal Work-Study Programs.

## 6 REFERENCES

### 6.1 *Project Work Plan*

The project work plan is documented on the following page.

ID	Task Name	Duration	Start	Finish	2004											
					Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar				
1	<b>Task Order 144 Period of Performance</b>	<b>116 days?</b>	<b>Fri 8/22/03</b>	<b>Sat 1/31/04</b>	[Gantt chart bar]											
2	Award task order	0 days	Fri 8/22/03	Fri 8/22/03	[Gantt chart bar]											
3	Kick-off meeting	0 days	Tue 9/2/03	Tue 9/2/03	[Gantt chart bar]											
4	<b>Support Activities (incl. bi-weekly status) - Ongoing</b>	<b>102 days</b>	<b>Tue 9/2/03</b>	<b>Thu 1/22/04</b>	[Gantt chart bar]											
5	Task Order Meeting	0 days	Tue 9/2/03	Tue 9/2/03	[Gantt chart bar]											
6	Task Order Meeting	0 days	Thu 9/4/03	Thu 9/4/03	[Gantt chart bar]											
7	Task Order Meeting	0 days	Mon 9/8/03	Mon 9/8/03	[Gantt chart bar]											
8	Task Order Meeting	0 days	Thu 9/11/03	Thu 9/11/03	[Gantt chart bar]											
9	Task Order Meeting	0 days	Mon 9/22/03	Mon 9/22/03	[Gantt chart bar]											
10	Task Order Meeting	0 days	Thu 9/25/03	Thu 9/25/03	[Gantt chart bar]											
11	Task Order Meeting	0 days	Mon 9/29/03	Mon 9/29/03	[Gantt chart bar]											
12	Task Order Meeting	0 days	Thu 10/2/03	Thu 10/2/03	[Gantt chart bar]											
13	Task Order Meeting	0 days	Thu 10/9/03	Thu 10/9/03	[Gantt chart bar]											
14	Task Order Meeting	0 days	Thu 10/16/03	Thu 10/16/03	[Gantt chart bar]											
15	Task Order Meeting	0 days	Wed 10/29/03	Wed 10/29/03	[Gantt chart bar]											
16	Task Order Meeting	0 days	Thu 11/13/03	Thu 11/13/03	[Gantt chart bar]											
17	Task Order Meeting	0 days	Thu 12/4/03	Thu 12/4/03	[Gantt chart bar]											
18	Task Order Meeting	0 days	Thu 12/18/03	Thu 12/18/03	[Gantt chart bar]											
19	Task Order Meeting	0 days	Thu 1/8/04	Thu 1/8/04	[Gantt chart bar]											
20	Task Order Meeting	0 days	Thu 1/15/04	Thu 1/15/04	[Gantt chart bar]											
21	Task Order Meeting	0 days	Thu 1/22/04	Thu 1/22/04	[Gantt chart bar]											
22	Task Order Meeting	0 days	Thu 1/29/04	Thu 1/29/04	[Gantt chart bar]											
23	PKI Pilot Meeting	0 days	Thu 10/2/03	Thu 10/2/03	[Gantt chart bar]											
24	Technology Meetings - Ongoing (As Required)	47 days	Thu 9/25/03	Fri 11/28/03	[Gantt chart bar]											
25	Policy Meeting	0 days	Mon 9/8/03	Mon 9/8/03	[Gantt chart bar]											
26	Credential Assessment Initial Meeting	0 days	Tue 9/30/03	Tue 9/30/03	[Gantt chart bar]											
27	Meetings with WebCAAF re: credential assessment framework	23 days	Mon 9/15/03	Wed 10/15/03	[Gantt chart bar]											
28	ED PIN Re-Engineering Review	24 days	Mon 9/15/03	Thu 10/16/03	[Gantt chart bar]											
29	8th Federal Education PKI Meeting	0 days	Tue 12/16/03	Tue 12/16/03	[Gantt chart bar]											
30	Task Order Modification	34 days	Mon 11/24/03	Thu 1/8/04	[Gantt chart bar]											
31	144.1.1 E-Authentication (E-Gov) Project Performance Report	20 days	Thu 12/4/03	Wed 12/31/03	[Gantt chart bar]											
32	Submit Deliverable 144.1.1 to FSA	0 days	Wed 12/31/03	Wed 12/31/03	[Gantt chart bar]											
33	FSA Feedback on Deliverable	0 days	Thu 1/15/04	Thu 1/15/04	[Gantt chart bar]											
34	<b>Revise Deliverable per FSA Feedback</b>	<b>6 days</b>	<b>Thu 1/15/04</b>	<b>Thu 1/22/04</b>	[Gantt chart bar]											
35	Add detail to project plan	6 days	Thu 1/15/04	Thu 1/22/04	[Gantt chart bar]											
36	Add detail to recommendations in White Paper	6 days	Thu 1/15/04	Thu 1/22/04	[Gantt chart bar]											
37	Resubmit Deliverable 144.1.1	0 days	Mon 1/26/04	Mon 1/26/04	[Gantt chart bar]											
38	<b>1. Comments on Emerging Documents</b>	<b>14 days</b>	<b>Mon 11/17/03</b>	<b>Thu 12/4/03</b>	[Gantt chart bar]											
39	NIST 800-63 Draft Recommendation for Electronic Authentic	7 days	Mon 11/17/03	Tue 11/25/03	[Gantt chart bar]											
40	Review Documentation	7 days	Mon 11/17/03	Tue 11/25/03	[Gantt chart bar]											
41	Comments provided to FSA	0 days	Tue 11/25/03	Tue 11/25/03	[Gantt chart bar]											
42	<b>E-Authentication Strategic Business Plan - DRAFT</b>	<b>8 days</b>	<b>Tue 11/25/03</b>	<b>Thu 12/4/03</b>	[Gantt chart bar]											
43	Review Documentation	8 days	Tue 11/25/03	Thu 12/4/03	[Gantt chart bar]											
44	Comments provided to FSA	0 days	Thu 12/4/03	Thu 12/4/03	[Gantt chart bar]											
45	<b>2. FSA Computer Matching Agreement (FSA)</b>	<b>104 days</b>	<b>Fri 9/5/03</b>	<b>Wed 1/28/04</b>	[Gantt chart bar]											
46	Support FSA tasks for CMA approval	102 days	Fri 9/5/03	Mon 1/26/04	[Gantt chart bar]											
47	Help understand approval process	10 days	Thu 1/15/04	Wed 1/28/04	[Gantt chart bar]											
48	Receive process documentation from FSA	0 days	Fri 1/16/04	Fri 1/16/04	[Gantt chart bar]											
49	Discuss process with Marya Dennis, FSA	0 days	Fri 1/23/04	Fri 1/23/04	[Gantt chart bar]											
50	Work with FSA to Summarize Actions/Next Steps	2 days	Fri 1/23/04	Mon 1/26/04	[Gantt chart bar]											
51	CMA Process Summary	0 days	Mon 1/26/04	Mon 1/26/04	[Gantt chart bar]											
52	<b>3. White Paper - FSA E-Authentication Position</b>	<b>42 days</b>	<b>Thu 12/4/03</b>	<b>Sat 1/31/04</b>	[Gantt chart bar]											
53	Prepare initial draft	20 days	Thu 12/4/03	Wed 12/31/03	[Gantt chart bar]											
54	Update white paper	20 days	Fri 1/2/04	Thu 1/29/04	[Gantt chart bar]											
55	Submit with Deliverable 144.1.2	1 day	Fri 1/30/04	Sat 1/31/04	[Gantt chart bar]											
56	<b>4. Credential Assessment Framework Support for ED PIN</b>	<b>88 days</b>	<b>Tue 9/30/03</b>	<b>Thu 1/29/04</b>	[Gantt chart bar]											
57	Support FSA activities	85 days	Tue 9/30/03	Mon 1/26/04	[Gantt chart bar]											
58	Propose high level tasks/objectives	0 days	Mon 1/19/04	Mon 1/19/04	[Gantt chart bar]											
59	Support FSA activities with assessment planning	8 days	Tue 1/20/04	Thu 1/29/04	[Gantt chart bar]											
60	<b>5. FSA-HHS E-Sign Pilot for Schools</b>	<b>85 days</b>	<b>Tue 9/30/03</b>	<b>Mon 1/26/04</b>	[Gantt chart bar]											
61	Support process	85 days	Tue 9/30/03	Mon 1/26/04	[Gantt chart bar]											
62	<b>6. EDUCAUSE/NIH/Higher Education Pilot Support</b>	<b>85 days</b>	<b>Wed 10/1/03</b>	<b>Tue 1/27/04</b>	[Gantt chart bar]											
63	Support activities	85 days	Wed 10/1/03	Tue 1/27/04	[Gantt chart bar]											
64	Document high level summary	0 days	Mon 10/6/03	Mon 10/6/03	[Gantt chart bar]											
65	<b>144.1.2 E-Gov E-Authentication Opportunities Support</b>	<b>21 days?</b>	<b>Fri 1/2/04</b>	<b>Fri 1/30/04</b>	[Gantt chart bar]											
66	Update White Paper	21 days?	Fri 1/2/04	Fri 1/30/04	[Gantt chart bar]											
67	<b>Document CMA Approval Process</b>	<b>6 days?</b>	<b>Fri 1/16/04</b>	<b>Fri 1/23/04</b>	[Gantt chart bar]											
68	Work with Marya Dennis/FSA	6 days?	Fri 1/16/04	Fri 1/23/04	[Gantt chart bar]											
69	Receive process documentation	0 days	Fri 1/16/04	Fri 1/16/04	[Gantt chart bar]											
70	Meeting with Marya Dennis	0 days	Fri 1/23/04	Fri 1/23/04	[Gantt chart bar]											
71	Summarize process	0 days	Fri 1/23/04	Fri 1/23/04	[Gantt chart bar]											
72	Help Review CAF Material	6 days?	Fri 1/16/04	Fri 1/23/04	[Gantt chart bar]											
73	Meeting with Schools, Data Strategy, etc.	10 days?	Mon 1/19/04	Fri 1/30/04	[Gantt chart bar]											
74	Prepare Deliverable 144.1.2	5 days?	Mon 1/26/04	Fri 1/30/04	[Gantt chart bar]											
75	Submit Deliverable 144.1.2 to FSA	0 days	Fri 1/30/04	Fri 1/30/04	[Gantt chart bar]											
76	<b>Future Considerations for FSA</b>	<b>3 days</b>	<b>Fri 2/6/04</b>	<b>Tue 2/10/04</b>	[Gantt chart bar]											
77	ED PIN Credential Assessment Kick-off Meeting	1 day	Fri 2/6/04	Fri 2/6/04	[Gantt chart bar]											
78	NIST Knowledge Based Authentication Symposium	2 days	Mon 2/9/04	Tue 2/10/04	[Gantt chart bar]											

## 6.2 Project Meetings

 <h1 style="text-align: center;">E-Authentication &amp; E-Signature Support</h1> <h2 style="text-align: center;">January 8, 2004</h2>	
<b>Attendees:</b> 9:30 a.m. At UCP	Neil Sattler – FSA Program Director Yateesh Katyal – Integration Partner/Accenture
<b>Purpose of Meeting</b>	Task Order weekly status meeting. <b>Agenda:</b> <ul style="list-style-type: none"> <li>▪ Task Order Modification – In process at FSA</li> <li>▪ Deliverable 144.1.1 – In FSA review</li> <li>▪ Work Streams                             <ul style="list-style-type: none"> <li>○ CMA</li> <li>○ HHS Pilot                                     <ul style="list-style-type: none"> <li>▪ Dependency upon E-Authentication Interim Architecture Update</li> </ul> </li> <li>○ E-Gov E-Authentication Emerging Documentation                                     <ul style="list-style-type: none"> <li>▪ Credential Assessment Framework (CAF)</li> <li>▪ Common Credential Assessment Profile</li> <li>▪ PIN Credential Assessment Profile</li> <li>▪ E-Authentication Strategic Business Plan</li> <li>▪ Interface Specs. For SAML Artifact Profile</li> <li>▪ NIST Sp. Pub. 800-63 (Recommendation for Electronic Authentication)</li> </ul> </li> <li>○ ED PIN Credential Assessment                                     <ul style="list-style-type: none"> <li>▪ Dependency upon CAF, Common Credential Assessment Profile, PIN Credential Assessment Profile, NIST 800-63, other?</li> <li>▪ Security Certification &amp; Accreditation</li> </ul> </li> <li>○ NIH-EDUCAUSE PKI Pilot                                     <ul style="list-style-type: none"> <li>▪ FSA CIO Interview</li> <li>▪ FSA Participation Decision   <ul style="list-style-type: none"> <li>• Potential Form(s)</li> </ul> </li> </ul> </li> <li>○ Additional E-Authentication Opportunities                                     <ul style="list-style-type: none"> <li>- White Paper</li> <li>- CMO</li> <li>- TPM</li> </ul> </li> <li>○ Other                                     <ul style="list-style-type: none"> <li>▪ Upcoming deliverable – 01/30/2004</li> </ul> </li> </ul> </li> </ul>
<b>Decisions Made</b>	N/A.
<b>Issues/Concerns</b>	N/A.

<b>Open Action Items</b>	N/A (task order modification in process).	
<b>Open Action Items from Previous Meeting(s)</b>	<ul style="list-style-type: none"> <li>▪ None.</li> </ul>	
<b>Discussion</b>	N/A.	
Next Meeting(s): 01/15/2004 9:30am	<ul style="list-style-type: none"> <li>▪ Weekly Task Order Status.</li> </ul>	

 <div style="text-align: center;"> <h2 style="color: red;">E-Authentication Pilot</h2> <h3>January 15, 2004</h3> <h3>Meeting Minutes/Action Items</h3> </div> 		
<b>Attendees</b>	Neil Sattler Yateesh Katyal	
<b>Purpose of Meeting</b>	Task Order weekly status meeting.	
<b>Open Action Items</b>	N/A.	
<b>Discussion Items</b>	<ol style="list-style-type: none"> <li>1. <b>Document &amp; Understand CMA Process</b> - Accenture to work with FSA SME to document CMA process. Meeting scheduled with Marya Dennis for Friday (23<sup>rd</sup>) @ 1:30pm. Marya suggested including Alexia Roberts from CIO.</li>   <li>2. <b>Review GAO PKI Report</b> - comments on "Information Security: Status of Federal Public Key Infrastructure Activities at Major Federal Departments and Agencies. GAO-04-157, December 15 <a href="http://www.gao.gov/cgi-bin/getrpt?GAO-04-157">http://www.gao.gov/cgi-bin/getrpt?GAO-04-157</a> Highlights - <a href="http://www.gao.gov/highlights/d04157high.pdf">http://www.gao.gov/highlights/d04157high.pdf</a>". The report is an excellent compilation of PKI initiatives within the Federal environment, the challenges as well as the strength of the technology. It highlights the 4 challenges as being policy and guidance, funding, interoperability, and training and</li> </ol>	

administration. The reports acknowledges strength of PKI technology over password-based systems – it does not, however, identify the limitations of the technology itself. The report lacks a discussion on alternatives where PKI is not an option for identification, authentication or electronic signature (e.g., business transactions with public citizens). The report also lacked a discussion of industry efforts where basic PKI capabilities are enabled as part of the operating system and the implications thereof. The report does provide a good discussion from the technical and policy perspective but lacks a discussion on business use. This is, perhaps, where GAO’s recommendation for a framework from OMB may be helpful. The conclusion states the framework will help with “consolidation of PKI technology across Government”; focus would be better served if the objective included interoperability standards between Government and private sector. Washington Technology ([http://www.washingtontechnology.com/news/1\\_1/daily\\_news/22526-1.html](http://www.washingtontechnology.com/news/1_1/daily_news/22526-1.html)), Government Computer News ([http://www.gcn.com/vol1\\_no1/daily-updates/24644-1.html](http://www.gcn.com/vol1_no1/daily-updates/24644-1.html)), other articles also report GAO findings.

3. **High Level Plan/Major Steps for ED PIN Credential Assessment**

– Accenture to provide key steps for ED PIN credential assessment. A high level plan with 12 steps is noted below:

- A. 01/16/2004 – Receive current CAF including PIN CAF and NIST 800-63.
- B. 01/20/2004 – Formulate FSA Executive Team for Credential Assessment.
- C. 01/20/2004 – Establish FSA Support Team for Assessment (resource allocation).
- D. 01/21 – 01/23/2004 – Seek lessons learned and best practices from assessment completed/underway by GSA.
- E. 01/21 – 01/30 – Collect/compile/update documentation, as necessary.
- F. 01/23/2004 – Review CAF requirements relative to the ED PIN.
- G. 01/26/2004 – Submit questions to GSA assessment team.
- H. 02/02/2004 – Kick-off meeting for ED PIN credential assessment.
- I. 02/03 – 02/06/2004 – ED PIN credential assessment (2 days).
- J. 02/05/2004 – ED PIN credential assessment debrief.
- K. 02/06/2004 – ED PIN credential assessment debrief – executive team.
- L. 02/06/2004 – Determine Next Steps.

4. **Deliverable 144.1.1 - Update Task Order Project Plan.** See updated draft plan.

5. **Deliverable 144.1.1 - Include comments on NIST e-authentication guidance in deliverable** – review comments included in meeting minutes for November 13, 2003. Comments included in Section 3.3.
6. **Deliverable 144.1.1 - Include comments on E-Authentication Strategic Business Plan** – Comments referenced in meeting minutes for December 4, 2003. Comments included in Section 3.3.
7. **Deliverable 144.1.1 - Include review comments for CAF** – comments included in Section 3.3.
8. **Deliverable 144.1.1 - Include recommendations for next steps in White Paper.** See updated White Paper.
9. **Broker meeting with Paul and Keith** to develop a walk around document for PKI. Need clarification; not complete.
10. **FSA will receive current information from GSA** (Mr. Sill).
11. **Candidate forms for PKI pilot.** FSA should select form in collaboration with the U.S. Department of Education and School customers. Potential candidates include:
  - P. ED 424 Form – Application Form for Federal Education Assistance
  - Q. ED 524 Form – Budget Information, Non-Construction Programs
  - R. ED 524-B Form – Grant Performance Report
  - S. ED 80-0013 Form – Certifications Regarding Lobbying; Debarment, Suspension and Other Responsibility Matters; and Drug-Free Workspace Requirements
  - T. ED 80-0014 Form – Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion – Lower Tier Covered Transactions
  - U. ED 80-0016 Form – Certification of Eligibility for Federal Assistance in Certain Programs
  - V. SF 424B Form – Assurances, Non-Construction Programs
  - W. SF LLL Form – Disclosure of Lobbying Activities
  - X. SAIG Enrollment Document
  - Y. Equity in Athletics Disclosure Act
  - Z. Fiscal Operations Report and Application to Participate in Opportunity Grant, and Federal Work-Study Programs
  - AA. Student Assistance General Provisions – Subpart K – Cash Management
  - BB. Federal Pell Grant Program Recipient Financial Management Systems (RFMS)
  - CC. Application for Approval to Participate in Federal Student

	<p>Financial Aid Programs DD. Fiscal Operations Report and Application to Participate (FISAP) in the Federal Perkins Loan, federal Supplemental Educational Opportunity Grant, and Federal Work-Study Programs.</p>		
<b>Agenda for next Meeting</b>	January 22, 2004		
<b>Contact</b>	<table border="0"> <tr> <td>Neil Sattler, Director Federal Student Aid U.S. Department of Education <a href="mailto:Neil.Sattler@ed.gov">Neil.Sattler@ed.gov</a> <a href="mailto:Yateesh.Katyal@Accenture.com">Yateesh.Katyal@Accenture.com</a> 202-377-3513</td> <td>Yateesh Katyal, Ph.D. Integration Partner Accenture  703-947-3510</td> </tr> </table>	Neil Sattler, Director Federal Student Aid U.S. Department of Education <a href="mailto:Neil.Sattler@ed.gov">Neil.Sattler@ed.gov</a> <a href="mailto:Yateesh.Katyal@Accenture.com">Yateesh.Katyal@Accenture.com</a> 202-377-3513	Yateesh Katyal, Ph.D. Integration Partner Accenture  703-947-3510
Neil Sattler, Director Federal Student Aid U.S. Department of Education <a href="mailto:Neil.Sattler@ed.gov">Neil.Sattler@ed.gov</a> <a href="mailto:Yateesh.Katyal@Accenture.com">Yateesh.Katyal@Accenture.com</a> 202-377-3513	Yateesh Katyal, Ph.D. Integration Partner Accenture  703-947-3510		

### 6.3 WHITE PAPER: *Develop an FSA E-Authentication, E-ID & E-Sign Business Plan*

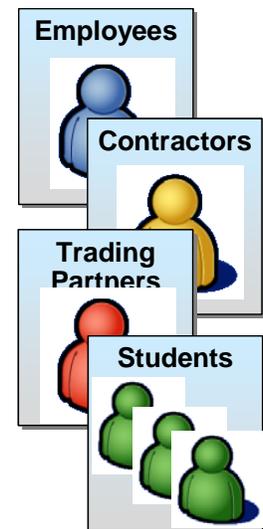
#### **Purpose**

The purpose of this White Paper is to communicate the need for an FSA enterprise-wide business plan to structure, strengthen and expand FSA leadership in E-ID, E-Authentication and E-Sign initiatives. The White Paper suggests specific actions that should be undertaken to continue an enterprise focus across multiple E-ID related initiatives. This White Paper discusses FSA Expertise, the Current Landscape, Anticipated Growth, Technical Infrastructure, Business Considerations and Opportunities. The specific actions suggested include near term, medium term and long term implementation opportunities.

Seven years of experience with the knowledge-based ED PIN credential now suggests the need for limiting it to Student use and examining other options for Trading Partners. A business plan is necessary to strengthen the current credential and associated technologies while introducing or examining other credential(s). Any change will need to be accomplished without disruption to current service.

#### ***FSA will Need Expertise Beyond the ED PIN to sustain E-ID, E-Authentication & E-Sign Leadership***

The CIO Office of Applications Development at the U.S. Department of Education (ED) Office of Federal Student Aid (FSA) has been at the forefront promoting *E-Authentication* as a key strategy for enabling e-Gov business goals. Having successfully developed and promoted the business case related to *E-Sign* (electronic signatures) for FSA customers, the Office of Applications Development implemented E-Sign for promissory notes in the Direct Loan, FFEL and Perkins programs as well as the FAFSA. The Free Application for Federal Student Aid (FAFSA) offers, since 1997, a completely paperless process to over 6 million annual applicants seeking financial aid. The catalyst for achieving rapid success has been the Office of Applications Development persistent and constant communication with its customers as well as business process owners to understand *E-ID* (electronic credential) requirements. Customer groups include students and trading partners (schools and financial partners - lenders, guarantee agencies, servicers, etc.). Business process owners span all FSA and certain external agencies (e.g., U.S. General Services Administration (GSA), Office of Management and Budget (OMB), E-Gov Initiatives, etc.). The FSA business process owners specifically include the Schools, Financial Partners and Students channels as well as the Office of General Counsel, Policy Development Division, and other support organizations. With over 2 Million E-Sign transactions a year and a user base of over 40 Million, FSA's progress is maturing to the next level. At this level, there is higher need for ensuring security, privacy and confidentiality associated with electronic transactions.

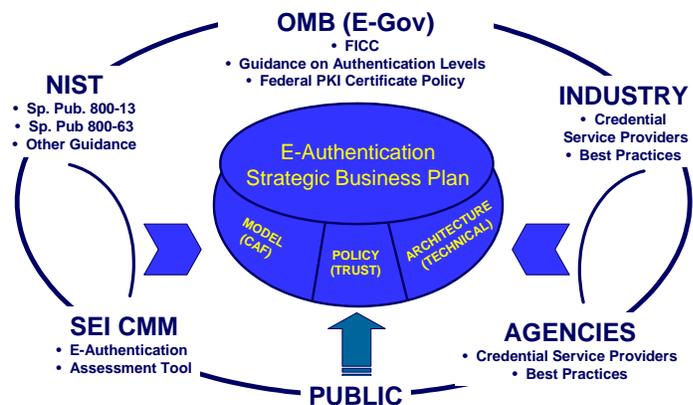


FSA is, and continues to be, sensitive to the security, privacy and confidentiality needs of communities it serves. Paperless alternatives are provided only as options to traditional processes; or as the only option, with agreement from the community. The security certification and accreditation process for its IT systems includes a focus on security, privacy and confidentiality. This focus will help FSA maintain

its leadership position as long as weaknesses related to electronic credentials are documented and adequately removed.

The IT systems at FSA are used by many groups including employees, contractors, trading partners, students, and others. While the ED PIN processes have been successful for E-ID, E-Authentication and E-Sign, there are currently few limitations regarding its applicability for a specific group(s). There are also 40 other authentication processes at FSA in addition to the ED PIN. The business, operational, technical, legal and political needs for an enterprise-wide Business Plan that provides guidance for managing electronic identity is very much necessary. Without such guidance there is a risk of contaminating the integrity associated with the ED PIN (and the over 40 other credentials) that will ultimately counter FSA's E-ID, E-Authentication and E-Sign success.

*FSA can Learn from, & Contribute towards, multiple Federal & Industry Initiatives* Significant investment in E-ID-related projects is being made by Federal organizations including OMB, NIST, and other agencies such as FSA, USDA, GSA, NIH, DHHS, etc. Industry attention from numerous organizations, credential service providers and standards groups as well as the Software Engineering Institute (SEI) is also focused on addressing E-ID, E-Authentication and E-Sign needs. Efforts resulting from Federal guidance, combined with industry standards such as the Liberty Alliance and FSA's own business experience are bound to yield best practices that will benefit many organizations including FSA. Not only will a business plan provide structure and direction, but it can also allow FSA with an opportunity to influence some of the emerging architectures, standards and technologies through its first-hand experience.

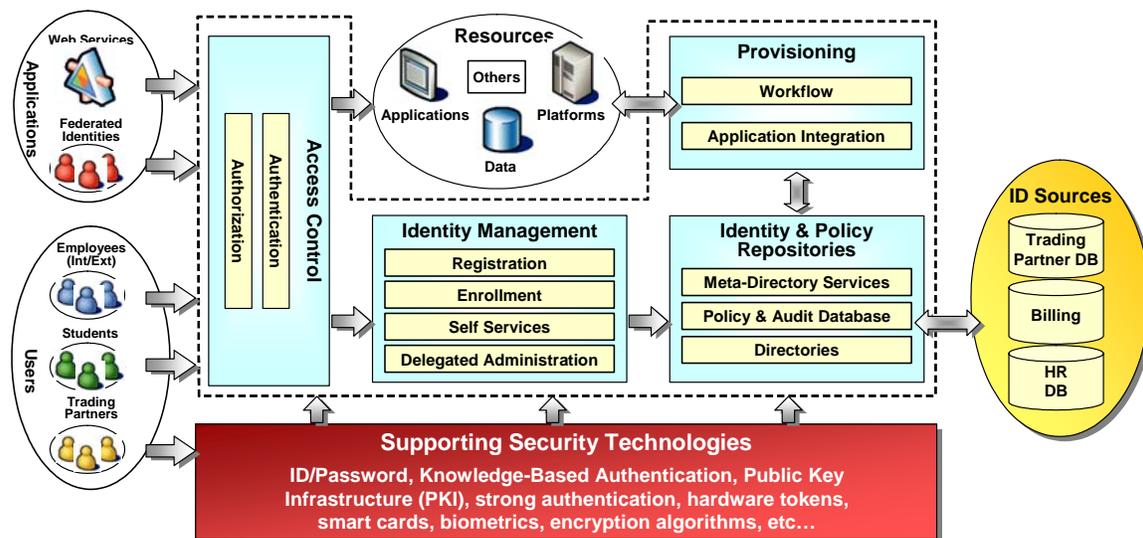


*No Turning Back - More Transactions will use the ED PIN* With over 6 Million new customers annually, the Opportunity Pipeline for FSA is remarkably rich. These new customers also provide incremental opportunities for electronic service during the financial aid life cycle - expecting to top 100 Million potential users by 2009<sup>1</sup>. Less than 5% of this user base currently takes advantage of E-ID, E-Authentication and E-Sign services. A very significant part of the responsibility for increasing market penetration lies with FSA and its ability to design a sound infrastructure that can continue to service customers while acquiring additional customers at increasing rates. While benefiting customers, these opportunities also provide FSA with the means to service more customers electronically and faster, using industry standards that cost less to integrate and operate, and provide levels of fraud detection and prevention capabilities that are impossible without an enterprise-wide identity management and authentication approach.

*FSA needs to Reduce the number of Customer Credentials* Most of the components for establishing an E-ID, E-Authentication and E-Sign business plan already exist at FSA, albeit duplicative. These include the Identity Management, Provisioning, Repository, Access Control and Interface functions used to manage, issue, store, and utilize the 40+ FSA customer credentials to enable

<sup>1</sup> Source: U.S. Department of Education - <http://www.ed.gov/offices/OUS/StudentLoanTables/index.html>

electronic transactions. Most FSA IT systems are electronically accessible (i.e., authentication), possess strong policies and rules for access control (i.e., authorization), comply with standards for system interfaces (i.e., application program interface - APIs, enterprise application integration - EAI connectors, web services, etc.), and provide customer support (i.e., help desk, web chat, etc.). Authentication is also one of the criteria for compliance with security certification and accreditation. FSA also has initiatives to link customer data and provide Single Sign-On<sup>2</sup> capability to ease the burden on customers. The focus on all these aspects of infrastructure is yet another reason for developing a business plan to understand the enterprise needs and guide future efforts. One such target enterprise-wide E-ID, E-Authentication and E-Sign architecture is illustrated below.



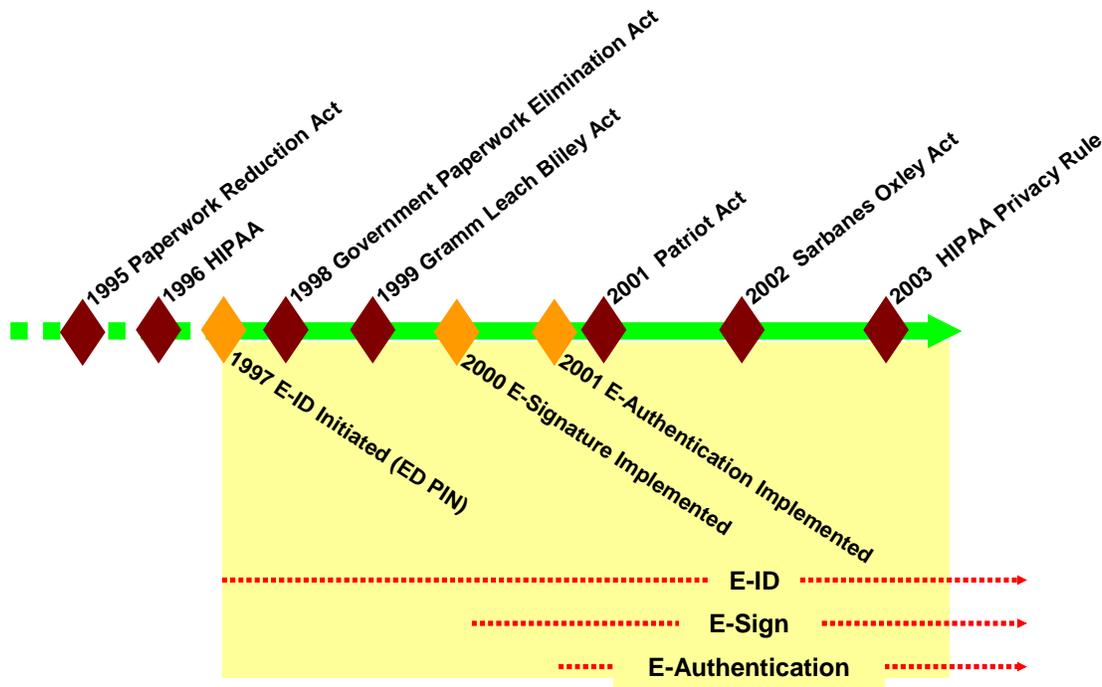
It is not the intent of this White Paper to recommend any architecture for FSA but simply to identify the need for a business plan containing elements identified above. As such, at this time the architecture above is for illustrative purposes only. The target vision should include E-ID as an objective.

*Knowledge-Based Authentication is Important to FSA* Any E-ID, E-Authentication and E-Sign business plan is likely to be unique to an organization. For example at FSA, there are opportunities to design solutions that can support at least 2 different types of customers - students and trading partners. The ED PIN is an excellent implementation for the student community and can be further strengthened using knowledge-based authentication and data management principles. Transitive trust approaches appear to be strong options for trading partner authentication. Transitive Trust Domains can allow flow of attributes to domains that trust them. Regardless, there are many methods that FSA should consider as part of developing an enterprise-wide authentication business strategy. Considerable federal and industry attention to identity management and authentication will also provide guidance on what and how FSA should approach the development of a strategy that includes these considerations (e.g., PKI and other strong authentication alternatives).

Other than technology, the development of a strategic E-ID, E-Authentication and E-Sign business plan will also need to address legislation. FSA has no issue in complying with legislation related to E-Sign

<sup>2</sup> One alternative should also include Reduced (as opposed to Single) Sign-On.

or E-Authentication processes. Initial efforts related to paperwork reduction and paperwork elimination legislation are now focused on privacy and security. The three work streams – E-ID, E-Authentication and E-Sign – help FSA focus on compliance activities easily.



Legal aspects, in addition to business issues and technological advances, will also need to be part of the broader guidance. Legislation focusing on privacy and accountability issues includes CPNI, HIPAA, Patriot Act, Gramm Leach Bliley, and Sarbanes-Oxley. Each addresses a particular impact area and has corresponding costs associated with its violation. The following table summarizes these legislative impacts.

Legislation	Impact Area	Violation Cost
Customer Proprietary Network Information (CPNI)	<b>Privacy</b> - Establishes criteria and restrictions for sharing customer information	No precedents have yet been set for violations. Punitive damages in the amount of potential revenue from the violation are plausible.
Health Insurance Portability and Accountability Act (HIPAA)	<b>Privacy and Security</b> - Establishes standard for transaction and information handling to ensure the security and privacy of personal information	Civil penalties: \$100 per violation to \$25,000 per person; Criminal penalties: limited to \$250,000 and a 10 year prison sentence
Patriot Act	<b>Audit and Reporting</b> - Establishes guidelines for enacting anti money-laundering programs and reporting transactions	Civil penalties: up to \$275,000 per violation; Criminal penalties: \$1 million and a 12 year prison sentence
Gramm Leach Bliley	<b>Privacy</b> - Establishes administrative processes as a requirement for broadening activities that financial institutions can partake	Civil penalties: up to \$100,000 per violation; Criminal penalties: \$100,000 and a 5 years in prison sentence
Sarbanes-Oxley	<b>Audit and Reporting</b> - Improve	Criminal penalties: various

Legislation	Impact Area	Violation Cost
	transparency through record retention and reporting of financially relevant information	punishments up to \$25 million fines and 25 years in prison

While Government agencies such as FSA are not directly affected by such legislation, compliance is still good practice.

*FSA needs to Strengthen its E-ID Management Plan with Governance, Controls & Partnership* Clearly a leader in E-ID, E-Authentication, and E-Sign, FSA needs to continue to strengthen and increase current service, design new options and contribute to similar industry and federal efforts. The success of FSA’s future E-ID efforts will depend on the following:

- Establishment of enterprise-wide E-ID Governance
- Implementation of Management and internal Controls
- Assessment of Alternatives in Cooperation with Customers and Federal/Industry Partners.

An explanation of each opportunity is provided below.

**I. GOVERNANCE - Establish enterprise-wide E-ID Governance**

FSA’s most known E-ID credential is the ED PIN. There are also dozens of other E-ID credentials used within FSA. Most of the other credentials are specific to business applications. There is also no segmentation of credentials based on customers or types of transactions. Furthermore, there is no central responsibility for issuance and management of E-ID credentials. With over 40 credentials being issued and managed concurrently, it is time for FSA to provide enterprise guidance and, more importantly, have the ability to monitor FSA E-ID efforts from an enterprise perspective. Failure to govern this capability will likely result in incompatible, non-standard customer identification schemes that are difficult to integrate and increasingly expensive to maintain. The specific responsibility, and outcomes, for the E-ID governance should include:

1. E-ID Architecture. The purpose of the architecture should be to communicate the vision to optimize number of credential solutions used within the FSA enterprise.
2. Standards. Another aspect of Governance should include the analysis and publication of accepted standards for deploying and implementing credentials regardless of application system, i.e., enterprise-wide.
3. Governance Process. A process should be established, implemented and used enterprise-wide for managing electronic identity and its application within systems. This process should include technical, administrative, investment, and monitoring oversight across all credentials used within FSA.

This governance body must have sponsorship and participation from the Department of Education to be effective.

**II. CONTROLS - Implement Management Controls**

The number of ED PIN credentials issued by FSA is projected to exceed 90 million by the end of this decade. Lack of management controls will likely compromise this credential. Any compromise of integrity associated with this credential, whether by FSA or one of its customers, will likely force an expensive data clean-up effort. The same controls should be implemented for all FSA credentials. Aspects for consideration include:

4. System Reports. System reports should be reviewed that highlight usage – who is using credentials through which applications, errors, changes, problems, security vulnerabilities, potential fraudulent activity, etc.
5. Internal Controls. The development of management controls should also proactively address potential risks and controls to mitigate those risks. An area relevant to E-ID is identity theft and fraudulent use of credentials. Others will need to be analyzed by FSA as part of this process.
6. Customer Strategy. As part of this process, FSA needs to establish appropriate credentials based on customer group. Alternatively, FSA may want to formally decide to use the ED PIN for various types of identification and authentication purposes by many different customer groups and mitigate against that risk. Either way, a decision from the enterprise perspective is warranted.

### **III. PARTNERSHIP - Assessment of Alternatives in Cooperation with Customers & Federal/Industry Partners**

Preparedness is key. Opportunities exist for FSA to focus its enterprise authentication strategy with a two-pronged perspective. One addressing needs of the large and expanding student community and the other for higher education institutions, financial institutions, states, etc. (trading partners). The student community (i.e., individuals) will likely continue with knowledge-based authentication (ED PIN is an example). FSA will need to support other alternatives for its organizational partners. PKI is one of those alternatives and FSA has an opportunity to “learn and assess” the technological implications to its business processes. A potential large role for PKI looms in organizations requiring strong authentication, electronic signature, data integrity and confidentiality as well as non-repudiation capabilities. Perhaps PKI will mature as its own X.509 implementation or as part of a Web Services framework integrated with operating systems. Successful PKI projects have always been conducted as a partnership of IT and business. FSA has an opportunity to organize an IT/business team to “learn and assess” the PKI technology with a NIH-funded EDUCAUSE proof-of-concept involving FSA customers<sup>3</sup>. This participation will require an organized IT/business partnership and the identification of one FSA form.

The NIH-EDUCAUSE PKI pilot is one of many opportunities that FSA has for examining the business relevance of PKI technology. This pilot is of particular significance since higher education institutions are piloting electronic signature using PKI with XML forms. While many Federal agencies offer PKI capability, FSA does not possess the capability.

---

<sup>3</sup> FSA customers include: University of California (Berkeley), University of Texas – Health Sciences Center, Dartmouth College, University of Virginia, University of Wisconsin (Madison) and University of Alabama.

PKI is expensive to implement. It is a very sophisticated and complicated technology to plan for, procure, implement, and manage. Participating in a proof-of-concept with others who are learning is the best way to learn the business implications of this technology. It is unlikely FSA will deploy PKI applications for its customers over the next two years. To be prepared, FSA should consider:

7. Risk Assessments. The purpose of risk assessments, especially from 3<sup>rd</sup> party organizations, helps establish credibility and identify weaknesses. An appropriate assessment should be undertaken in the near term and repeated periodically.
8. Future Options. The ED PIN is unlikely to serve all enterprise identification, authentication and signature needs for the future. Given the various industry and federal efforts underway to examine technologies and their appropriate business uses, FSA should avail of opportunities to participate in studies that will specifically enable its future vision.
9. Implementation. Ultimately, the enterprise-wide implementation needs to implement options that mitigate business risks. This may result in a tiered approach where more than one technology is applicable.

FSA has been communicative with all its customer groups to understand their requirements and provide innovative business solutions. Continuing this tradition of communication and partnership with customers, other Federal initiatives (e.g., E-Gov) and industry groups should also be an important part of the strategic E-Authentication business plan. Organizations focused on promoting higher education interests such as EDUCAUSE are also important partners with FSA. This type of communication is important to any implementation.

The various opportunities discussed above are summarized in the table on the following page.

<b>OPPORTUNITIES</b>			
	<b>GOVERNANCE</b>	<b>CONTROLS</b>	<b>PARTNERSHIP</b>
<b>SHORT TERM</b> ( ~ 3 - 6 Months)	<u><b>ARCHITECTURE</b></u> Develop E-ID Architecture for FSA to Standardize on Credentials Used	<u><b>SYSTEM REPORTS</b></u> Develop Management and System Reports to Identify Problems and Improve ED PIN Data Integrity	<u><b>RISK ASSESSMENT</b></u> Demonstrate ED PIN Strength, Integrity & Trust Through 3 <sup>rd</sup> Party (NIST-Based) Assessment(s)
<b>MEDIUM TERM</b> (~6 - 12 Months)	<u><b>STANDARDS</b></u> Develop Enterprise-Wide E-Authentication Standards & Guidance	<u><b>INTERNAL CONTROLS</b></u> Develop Internal Controls to Detect & Prevent Fraud/Identity Theft	<u><b>FUTURE OPTIONS</b></u> Learn about and Assess Other Options with Other Federal Partners: <ul style="list-style-type: none"> <li>• PKI</li> <li>• Vendors &amp; Sourcing</li> <li>• Trust Models</li> <li>• Deployment Modes</li> </ul>
<b>LONG TERM</b> (~12 - 36 Months)	<u><b>GOVERNANCE PROCESS</b></u> Institute Governance Model for Architecture (how) & Standard Infrastructure (tools) for Enterprise Applications	<u><b>CUSTOMER STRATEGY</b></u> Develop Customer-Specific E-ID Strategy for Individuals and for Organizational Entities	<u><b>IMPLEMENTATION</b></u> Develop a Tiered Approach to electronic signature based on Business Risk

\* \* \* \* \*

## *6.4 Computer Matching Agreement (CMA) Process Documentation*

**BASIC PROCEDURES**

**COMPUTER MATCHING AGREEMENTS (CMA)**

<b>When</b>	<b>18 MONTH CMA</b>	<b>Time Needed</b>
8 Mos Before Expiration	<b>1.</b> Contact OPE (Dan Madzellan) and request a cost benefit analysis. (see attached)	1-2 mos.
7 Mos Before Expiration	<b>2.</b> Review and update current CMA, Federal Register Notice and Letters to Congress/OMB and create a draft for circulation. Check with PLI (Dan Klock) for significant changes. Contact other agency to discuss significant changes before drafting.	1 week
	<b>3.</b> Contact the other Agency to verify contact, estimate of timeline, corrections to contact info and or signature block and any other concerns. Ask if their OGC will do an unofficial review of doc before signatures.	
6 Mos Before Expiration	Circulate first draft of CMA, Cost Benefit Analysis, Letters to Congress/OMB, and Federal Register Notice to ED internal reviewers: PLI (Dan Klock, Bernardine Hayes), OGC (Debbie Friendly, Harold Jenkins (Program Attorney)), OCIO (Alexia Roberts), APPS (Ida Mondragon), APPS Security (Jacky Strickland). All issues must be resolved and the agreement approved before the letters can be completed.	
	The draft is attached to an e-mail indicating the names of the agencies, the expiration date of the current CMA and the date the review is due back to Marya.	
	Reviewers are given a deadline date to return any comments.	2-3 weeks

3 Wks Later (5 Mos before Ex)	Incorporate changes from reviewers and work to resolve any issues.	1 month
1 Month Later (4 Mos before Ex)	Circulate draft with changes to PLI, OGC, OCIO, APPS staff above.	1 week
1 Week Later	Incorporate changes to documents and finalize draft	1 week
	If other Agency will do an unofficial review, email draft to them. Request minimal turnaround time. 7-10 days. Incorporate changes from unoffical review.	10 days
	Send Federal Register Notice to Leslie Somerville in Division of Regulatory Services (DRS)	
1 Week Later (3.5 Mos before Expiration)	Update the Routing Slip/correspondence summary. Attach it to the package. Forward two originals of the final documents (CMA, CBA, Fed Register Notice, Letters to Congress) through the approval chain: (APPS: Sherlene, Bill, Jeanne, Mary K, Jennifer Douglas, Kay Jacks, PLI: Dan, Jeff, OCIO: Matthew Boggs, Debbie Price, Teri Shaw) for signature.	1 week +
	If Federal Register notice is in the pkg, it has to be cleared by DRS before Matthew Boggs will forward pkg to Debbie Price/Terri Shaw.	
	Send an electronic copy of CMA to Matthew Boggs to make corrections.	

	Remove the Federal Register Notice and the Letters to Congress from the pkg. Marya hand carries package to other Agency for signature process. And, picks it up when completed.	
<b>2 Mos Before Expiration</b>	Marya sends letters to Congress/OMB text to Alexia, notifies Alexia of the letter date. Alexia puts text on letterhead, dates and sends them.	2 days
Prior to 40 days before Expiration	When the other agency returns the signed documents, hand carry to ED's Data Integrity Board for approval. Both DIBs sign the certification page of the CMA.	
	Make copies for my file, Ida, Dan Klock (?)	
	Send 1 signed copy to Alexia Roberts (?)	

When	Preparation of the Federal Register notice	Time Needed
6 Mos Before Expiration	Prepare draft Federal Register notice. Refer to CMA file for previous notices and language. Hold it for comments from OGC, etc.	1 week +
4.5 Mos Before Ex	Request initial review from PLI (Dan Klock) prior to forwarding to the Division of Regulations Management (DRM).	1 week
1 Wk Later	Incorporate any changes (re Fed Register) from PLI into FR	5 days
1 Wk Later (4 Months Before Ex)	Email the draft to Leslie Somerville, Division of Regulations Management (DRM) (ED).	2-3 wks

2-3 Wks Later	Receive comments from DRM attorneys. Incorporate changes.	1 week
1 Week Later (3 Months Before Ex)	E-mail final to coordinator for approval to print in Fed Register. If changes are substantive a final could be circulated among ED staff. Print their final for publication.	2-3 weeks
2-3 Weeks Later (2 to 2.5 Months Before Expiration)	Forward final document for signatures (if it is not in the CMA pkg) to: Apps Processing (Sherlene, Bill, Jeanne, Mary K, Jennifer Douglas, Kay Jacks) PLI (Dan, Jeff), OCIO (Tom Pestka) & COO (Matthew Boggs, Debbie Price, Terri Shaw, ) Attach a completed correspondence summary. Check with COO re time needed for signature.	2-2.5 wks Tot: 1 for Apps & PLI, 1.5 for COO.
2-2.5 Wks Later 1.5 to 2 Months Before Ex)	Forward signed copy to DRM Coordinator (in FB6) for publication in the Federal Register. CIO will send for Publication.	1-2 Wks
1-2 Wks Later (1 to 1.5 Months Before Ex)	The coordinator will advise Marya when the Fed Register will be published. Comment has 30 day Comment Period.	30 day Comment Period
	Comments are sent to Marya.	

When	12 Month Agreement Renewal	Time Needed
4 Mos Prior to Expiration	1. Call the other Agency re: time it will take them to review and sign, unsubstantial changes (e.g. contact info, signature block).	
	2. Prepare the 12 Month CMA renewal document from prior agreement and update the correspondence summary sheet.	
	3. Send electronic copies of the CMA renewal document to Dan Klock and Debbie Friendly. Give them 5 days for review and comment.	1 Week
3.5 Mos Prior to Expiration	Incorporate changes from #3 above.	
Within 3 Mos of Expiration	Forward two CMA renewal documents and 1 copy of the current CMA and all it's attachments (CBA, FR Notice, Letters to Congress) for clearance (Sherlene, Bill, Jeanne, Mary K, Jennifer, Kay Jacks, Dan Klock, Matthew Boggs, Debbie Price and Terri Shaw. Attach the correspondence summary sheet. Call and follow up as needed.	2-2.5 Weeks
2-2.5 Weeks (2 to 2.5 Mos Before Ex)	Upon receipt of the signed renewals, Marya hand carries them to the other Agency for Program Official and DIB signatures. Call and follow up as needed.	1 to 4 Weeks
1 to 4 Weeks Later	When the other agency has signed the renewals, Marya hand carries them to ED's DIB for approval.	2 Weeks
	Make copies for Ida, my file, Dan Klock (?)	
	Send original to Alexi Roberts (?)	

