



**SFA Modernization Partner
United States Department of Education
Student Financial Assistance**

**Office of Chief Information Officer
Innovations Division
FFELP Digital Signature White Paper**

Final Version

October 10, 2000



Executive Summary

This white paper explores the opportunity for SFA to engage in a digital signature pilot for students signing the Federal Family Educational Loan Program (FFELP) Master Promissory Note (MPN). Specific objectives of this white paper are to:

- Describe the recently enacted legislation that enables the use of digital signatures
- Differentiate electronic signatures from other forms of electronic identification
- Outline the issues, concerns and risks the FFELP constituencies face by adopting the use of digital signatures
- Recommend a future course of action
- Define the business case for use of electronic signatures in FFELP
- Obtain management support for a FFELP digital signature pilot initiative

SFA is trying to support business process transitions into electronic environments. The national legislative foundation is being established. The necessary technological capabilities are being developed. However, SFA may not be ready to move to a digitally signed MPN due to the following concerns:

- the lack of an identity proofing standard (E-Identification)
- digital signatures legal enforceability case law
- a clear mechanical understanding of PKI in the FFELP process

This white paper explores these issues and proposes the approval of a pilot program to pursue remedies to these issues. Specifically, this white paper recommends a pilot program to test the feasibility of using Public Key Infrastructure (PKI) and digital signatures to electronically sign a FFELP MPN.

The USPS PKI/digital signature solution is a product alternative that delivers superior identity proofing capabilities, external operability opportunities and significant fraud enforcement authority. SFA should pursue the electronic signing of the FFELP MPN using this product because the constituents involved in the process (namely the student, the Department, the educational institutions, and the lender) could all realize savings in cost and time by diminishing the dependence on “wet” signatures. The short and long-term benefits for the constituents involved are substantial. Moreover, the use of PKI adheres clearly to the goals of SFA by increasing customer and employee satisfaction and reducing costs.

SFA is not currently ready to support “wholesale” use of digital signature use for the FFELP and FDLP promissory note process. Before proceeding with this effort, or any of the proposed eSignature pilots, several actions must be completed. Next steps include:

- Review current regulations and determine if regulatory changes or supplemental guidance is needed
- Issue a FFELP “Dear Partner” Letter outlining SFA’s current position, desire to do a digital signature pilot, and ask for pilot proposals
- Move forward with a pilot

Advances in PKI technology, coupled with Federal acceptance of digital signatures as legally binding contracts, have created a favorable environment for exploring the possibility of incorporating digital signatures into the FFELP process. The Management Council should support the Innovations Division as we proceed with this pilot initiative.

<u>1</u>	<u>Introduction</u>	1
<u>2</u>	<u>Purpose and Objectives</u>	1
<u>3</u>	<u>Business Case for Change</u>	1
<u>4</u>	<u>Types of Electronic Authentication</u>	3
<u>4.1</u>	<u>Non-Cryptographic Methods</u>	3
<u>4.1.1</u>	<u>Personal Identification Numbers or Passwords</u>	3
<u>4.1.2</u>	<u>Personal Uniform Resource Locator (URL) using Secure Socket Layer (SSL)</u>	4
<u>4.1.3</u>	<u>Smart Card</u>	4
<u>4.1.4</u>	<u>Digitized Signature</u>	4
<u>4.1.5</u>	<u>Biometrics</u>	4
<u>4.2</u>	<u>Cryptographic Control Methods</u>	5
<u>4.2.1</u>	<u>Shared Symmetric Key Cryptography</u>	6
<u>4.2.2</u>	<u>Public/Private Key (Asymmetric) Cryptography & Digital Signatures</u>	6
<u>5</u>	<u>Why Digital Signatures?</u>	8
<u>5.1</u>	<u>Writing and Signature Requirements</u>	8
<u>5.2</u>	<u>Digital Signature Standards</u>	9
<u>5.2.1</u>	<u>Authenticity</u>	9
<u>5.2.2</u>	<u>Data Integrity</u>	9
<u>5.2.3</u>	<u>Non-repudiation</u>	9
<u>5.2.4</u>	<u>Confidentiality</u>	10
<u>5.3</u>	<u>Supporting Digital Signatures with Public Key Infrastructure</u>	10
<u>5.3.1</u>	<u>Providing Authenticity</u>	10
<u>5.3.2</u>	<u>Providing Confidentiality</u>	10
<u>5.3.3</u>	<u>Providing Non-repudiation</u>	11
<u>5.3.4</u>	<u>Providing Data Integrity</u>	11
<u>6</u>	<u>Current FFELP Loan Requirements and Business Processes</u>	12
<u>7</u>	<u>FFELP Loan Requirements and Business Processes Using Digital Certificates</u>	14
<u>7.1</u>	<u>Student</u>	16
<u>7.2</u>	<u>Educational Institution</u>	16
<u>7.3</u>	<u>Lender and Guarantor</u>	16
<u>7.4</u>	<u>Department of Education</u>	16
<u>7.5</u>	<u>Certification Authority and Identification Proofing Authority</u>	17

8	<u>Digital Signature Options</u>	18
8.1	<i>Operational Considerations</i>	18
8.1.1	<u>Web browser vs. Smart Card</u>	18
8.1.2	<u>Identity Proofing</u>	18
8.1.3	<u>Storage of Digital Signature Results (eNote)</u>	19
8.1.4	<u>Lookups – One Time vs. Many</u>	19
8.2	<i>Operational Alternatives</i>	19
8.2.1	<u>Verisign</u>	19
8.2.2	<u>ACES</u>	19
8.2.3	<u>USPS</u>	20
8.3	<i>Summary</i>	20
8.3.1	<u>Feature Comparison</u>	20
8.3.2	<u>Cost Comparison</u>	21
8.3.3	<u>Differentiation</u>	21
8.3.4	<u>Recommendation</u>	21
9	<u>Risks, Issues and Concerns</u>	22
9.1	<i>PKI Risk Categories</i>	22
9.2	<i>PKI Issues and Concerns</i>	23
9.3	<i>PKI Risks by Constituencies</i>	27
10	<u>Next Steps</u>	29
10.1	<i>Review of Regulatory and Policy Parameters</i>	29
10.2	<i>Inform FFELP Partners</i>	29
10.3	<i>FFELP Digital Signature eMPN Pilot</i>	30
	<u>Appendix A – Review of Recent Legislation</u>	31
	<u>Appendix B – Current FFELP Prom Note Process</u>	36
	<u>Appendix C – An Example of Using the Digital Signature Process</u>	38
	<u>Appendix D – X.509v3 Digital Certificate Fields</u>	41
	<u>Appendix E – Digital Signature Proposal Evaluation Issues</u>	42

1 INTRODUCTION

The Federal Family Education Loan Program (FFELP) process is becoming less paper-based and more electronic. This paper explores a digital signature option for the FFELP's Master Promissory Note (MPN) wet signature requirement. A digital signature option would replace the current paper-based MPN and allow for completely automated on-line loan processing. This paper recognizes that a non-electronic MPN alternative must remain for those institutions unable to support total electronic processing.

Recent legislation and technology advances have made the use of a digital signature option credible, feasible and by some interpretations mandated¹. SFA is currently looking at many electronic identification/authorization initiatives. For example, the Federal Direct Loan Program (FDLP) loan origination and consolidation business processes are exploring PIN-based models for electronic signatures. This white paper explores the issues surrounding digital signatures and possible opportunities to employ public key infrastructure (PKI). By laying the foundation to understand PKI, the Student Financial Assistance (SFA) is now poised to take the next and significant step to achieve electronic processing of MPNs.

¹ GPEA requires Federal agencies, by October 21, 2003, to allow individuals or entities that deal with the agencies the option to submit information or transact with the agency electronically. Office of Management and Budget, "Implementation of the Government Paperwork Elimination Act."

2 PURPOSE AND OBJECTIVES

This white paper presents the results of the SFA Innovations Division investigation into the possibility of implementing digital signatures on FFELP master promissory notes (MPN). The white paper explores the possibilities the law has opened up and the opportunities technology now makes possible to streamline the FFELP process. Specific objectives of this white paper are to:

- Describe the recent legislation that enables the use of digital signatures;
- Differentiate electronic signatures from other forms of electronic authentication;
- Outline the issues, concerns and risks the FFELP constituencies face by adopting the use of digital signatures;
- Recommend a future course of action;
- Define the business case for use of electronic signatures in FFELP; and,
- Obtain management support for the Digital Signature Pilot Initiative

In the sections below, this paper describes a modified process that takes into consideration the burdens of each constituent, the costs involved, and the benefits of proceeding with this model. In addition, the paper addresses the specific concerns of SFA including:

- What level of proofing is acceptable?
- How will the digital signature be inserted into the FFELP process?

3 BUSINESS CASE FOR CHANGE

The business case for change is the SFA's desire to make all federal student aid processing easier for students, schools, loan originators and servicers, guaranty agencies, and the Department of Education (ED). Today, students can apply for financial aid electronically through the Free Application for Federal Student Aid (FAFSA) web site. Students, schools and lenders review the Student Aid Reports and Intuitional Student Information Record (ISIR) electronically. However, lenders require a student's written signature on master promissory notes (MPN) prior to any funds being released to schools. Providing a digital option to the MPN signatory requirement would result in an electronic MPN.

Digital signatures are an eSignature alternative that provide strong security and privacy features. The signing of the *Electronic Signatures in Global and National Commerce Act* in June 2000 and the wide availability of commercially available electronic signature solutions have made a completely electronic process now realizable. The digital signature, when combined with Public Key Infrastructure, offers authentication, data integrity, technical non-repudiation and confidentiality, whereby the sender cannot deny sending an electronic message, nor can the recipient deny its receipt.

Students benefit in a variety of ways from total electronic processing. Primarily, total electronic processing will result in approvals and disbursements that can be measured in days, not weeks. Also, the digital certificate could introduce the student to a new technology that has numerous applications allowing for expanded services at potentially reduced costs. Students separated by the oft-mentioned "digital divide" would become empowered - facilitated by ED - and delivered into an electronic world that would offer opportunities for access.

Schools benefit from using digital certificates by improving the financial aid process and the additional benefit of using this acquired digital signature capability in future applications. In instances where a signature is required, the school would have the ability to introduce a "digital signature" option. The potential cost savings for the school could be applied in various ways, but ultimately the school will determine its own methodology for reallocating the cost savings. The time savings would allow financial aid administrators to spend more time on those students who require more "hands-on" assistance.

Loan originators and servicers as well as guaranty agencies benefit by reducing costs and processing time. Lenders who embrace the use of digital signatures could reduce their application processing costs, as well as reduce their processing time from weeks to hours.²

ED benefits by continuing to deliver improved products for the stakeholders in the FFELP process and meet its legislative mandate to provide a reduction in paperwork. According to the *Government Paperwork Elimination Act (GPEA)*, the Department has the added responsibility to ensure a smooth and cost-effective transition to an

² Housing analysts said application fees are on average about 0.7 percent of the total loan size. So, on a \$100,00 loan the \$700 of application fees could be cut in half to \$350 as more lenders adopt total electronic processing of home loan applications. Rozens, Alekandrs, "E-signatures mortgage cost savings not seen soon," *Reuters*, July 6, 2000.

electronic government that provides improved service to the public. Further, the GPEA requires agencies to be able to conduct business with individuals and organizations and store records electronically by October 21, 2003.³

In general, PKI digital certificates offer at least equal, if not better, security and identification for electronic note signing that our current business process offers.

³ For a discussion of GPEA, OMB Procedures and Guidance on Implementing the GPEA, and the Electronic Signatures in Global and National Commerce Act see Appendix A.

4 TYPES OF ELECTRONIC AUTHENTICATION

The American Bar Association's Science and Technology Information Security Committee states that a signature must have the following attributes:⁴

- Signer authentication – should indicate who signed a document, message or record and [it] should be difficult for another person to produce without authorization
- Document authentication – should identify what is signed, making it impracticable to falsify or alter either the signed matter or the signature without detection.

Signer authentication and document authentication are tools used to thwart impersonators and forgers. These tools are essential components of electronic authentication.

Electronic authentication is defined as the assurance that an entity is who it claims itself to be. There are a number of methods available for providing electronic authentication and identification. Security experts agree that effective systems employ at least two or more of these strategies or factors to provide the best possible security solution. Clearly, multi-factor systems are more burdensome for the user (more tasks need to be completed before the authentication process is finished). However, the security benefit is that impersonation attacks become much more difficult (the would-be impersonator needs, for example, to know your password, imitate your typing style, and borrow your thumb without you knowing about it—all at the same time).

These factors mentioned above can be divided into four categories:⁵

- Something you have (such as a smart card or a hardware token)
- Something you know (such as a password or a PIN)
- Something you are, or something intrinsic to your body (such as a thumbprint or a retinal scan)
- Something you do (such as your typing characteristics or handwriting style)

The Office of Management and Budget (OMB) breaks electronic authentication into two types; non-cryptographic methods and cryptographic control methods.⁶ The proceeding sections are structured in the same way.

4.1 Non-Cryptographic Methods

Non-cryptographic methods rely solely upon an identification and authentication mechanism that must be linked to a specific software platform for each application. Whether or not these methods are encrypted at the time they are used is dependent upon the application and system being used. There are a number recognized methods: Personal Identification Numbers, Smart Cards, Digitized Signatures, and Biometrics.

4.1.1 Personal Identification Numbers or Passwords

Personal Identification Numbers (PINs) and passwords have been used to authenticate users since the creation of the social security account number. This type of authentication occurs when the user possesses a “shared secret,” something known to both the user and the system. Identification proofing is accomplished when the user is given/assigned their “shared secret.” Authentication is performed when the user inputs the shared secret and the application validates the secret against its database and thereby “authenticates” the user.

⁴ **Digital Signature Guidelines, American Bar Association Information Security Committee Science and Technology Section**

⁵ **Carlisle Adams and Steve Lloyd, Understanding Public Key Infrastructure, MacMillan Technical Publishing**

⁶ **OMB, Implementation of the GPEA – procedures and guidance, May 2, 2000.**

4.1.2 Personal Uniform Resource Locator (URL) using Secure Socket Layer (SSL)

A personal URL is a user interface into a web-based system. The URL is known only to the application and the user. Identification is established when the student requests access. The student's PIN and personal URL are mailed separately to the address provided by the student. To provide authentication and authorization, the URL is protected by either a PIN or password. In addition, the user's internet session is transmitted using SSL or an equivalent secure session standard. SSL uses a combination of public key cryptography (discussed in section 5.2) and symmetric cryptography to automatically encrypt information as it is sent over the Internet by the user and decrypt it before it is read by the intended recipient.

4.1.3 Smart Card

A smart card is a plastic card containing an embedded integrated circuit (IC) chip that can generate, store, or process data. With this technology the authentication method is built into the chip on the card. A smart card can be used to facilitate various authentication methods within the same card. To access the information on the card, the user interfaces with a Universal Serial Bus (USB) token (card reader).

By having different authentication choices the user can select the authentication technique that meets, but does not exceed, the information requirement for the transaction. One authentication approach is to provide information from the card's chip to the computer only when the user enters their PIN, password or biometric identifier. For example, if PIN is the preferred authentication method, the user swipes or inserts their card into a reader and enters their PIN. Using the identity information stored on the card combined with the PIN, the IC of the card performs the authentication process. Once the authentication is complete the required information can be transmitted from the card to the system. This option offers more security than just the use of a PIN, since the "shared secret" is between the user and the card, and the PIN data is not transferred from the smart card to a device or system.

4.1.4 Digitized Signature

A digitized signature is a graphical image of a handwritten signature. Most applications require that a user input their written signature using a digital pen and pad. Once the signature is digitized by the system, it may then be used by recognition software to compare a signature to the stored digitized signature. The digitized signature is considered more reliable than the PIN or password because it employs a biometric component to the creation of the image of the handwritten signature. The biometric elements of a digitized signature that make it unique are the measurements of how each stroke is made – duration, pen pressure, etc. This type of authentication requires the use of digital pen and pad or smart card technology in order to implement the solution.

4.1.5 Biometrics

Biometrics make use of the unique physical characteristics of individuals, by converting these characteristics into digital form and then interpreting them by computer at the time of authentication. Today, biometrics are being used and evaluated to provide even a higher degree of confidence of identification and authentication. However, the use of biometrics for authentication does raise the concern for the protection of a user's privacy. Because of this concern, it is recognized that biometrics are best suited for authentication to devices not for access to software systems over open networks.

Comparison of Non-Cryptographic Methods

	Password/PIN	Personal URL with PIN & SSL	Smart Card	Digitized Signature	Biometrics
Definition	Shared secret	Personal web page activated with PIN and generated during SSL session	Integrated Circuit (IC) on a card, usually no larger than a credit card	Graphical image of a handwritten signature	Conversion of individual characteristics into digital form to be interpreted by a computer
Examples of Use	FAFSA web site ATM Multiple Commercial Applications	Commercial Intranet Portals (i.e., Yahoo!, WebMD)	ED badge Metro	UPS FEDEX Sears	Dept of Defense
Vulnerabilities	PIN database User protection of PIN Passwords can be easily defeated	URL alone	PIN must be kept separate from card	Signature file must be protected	Privacy issues
Other considerations	Recommend encryption prior to use over an open network	Recommend use of PIN or password to activate session with SSL session	Used to employ one of the other security methods	Requires external equipment	Recommend encryption prior to use over an open network Use a third party to obtain verification. Best suited for access to systems not authentication to software systems
Positives	Easy to use	Personalized service	User authenticates to the card, not the network or device.	More reliable than a PIN because of the biometric component	Very difficult to circumvent
Negatives	Another PIN to remember	Requires storage space for each approved user	Requires a card reader.	Requires storage of the signature	If compromised a new biometric identifier may have limitations
Customer Acceptance	Proven	Proven	Proven but limited application	Proven but limited application	Proven but limited application

4.2 Cryptographic Control Methods

Unlike the non-cryptographic methods outlined above, cryptographic control methods use cryptography to authenticate identity. There are two cryptographic control methods: shared symmetric key and public/private key cryptography.

4.2.1 Shared Symmetric Key Cryptography

Symmetric Key Cryptography is also referred to as “Single-Key” cryptography. This method uses a single shared key to both encrypt and decrypt a message. It is important to note that the security of symmetric key encryption depends upon the secrecy of the key, not the secrecy of the algorithm used to create the key. Since the same key does two functions, it must be transferred from the signer to the recipient of the message. Naturally, manual delivery of the “Single-Key” is the optimum solution for the transfer of the key. Inherent in the use of single-key cryptography is risk of compromise. Because the possibility of compromise grows as the single key is passed from originator to each new receiver, who now has access to and the ability to use the originator’s single key.

4.2.2 Public/Private Key (Asymmetric) Cryptography & Digital Signatures

As the name implies public/private key cryptography differs from single-key cryptography because each user now has both a private key and public key. The whole system that implements public/private key architectures and allows them to be used with specific programs to offer secure communications is called a Public Key Infrastructure (PKI). As the names suggest, the public key is made public for others to use, while the private key is known only to its owner. A general-purpose public-key cryptographic algorithm relies on one key for encryption and a different but related key for decryption.

A “digital signature”

- is created when the owner of a private key uses that key to create a unique mark on an electronic document or file
- the recipient uses the owner’s public key to validate that the signature was generated with the associated private key
- because the public and private keys are mathematically linked, the pair is unique
- only the public key can validate signatures made using the corresponding private key
- the signature can be said to be unique to the owner, if the private key has been protected by the owner.

It is important to understand that the use of public/private keys to produce a digital signature offers no protection of confidentiality, since anyone who receives the message can decrypt the message using the sender’s public key. However, third-party solutions do exist that provide both a digitally signed document as well as encryption of the message from the sender to the receiver.

Although the public/private key approach is convenient and easy to use, there is one significant drawback – anyone could forward a public key claiming to be someone they are not. The solution to this problem is the public-key certificate.

A public-key certificate consists of:

- the public key
- the user ID of the key owner
- the verification of an independent trusted third party – the Certificate Authority (CA).

The CA is similar to an online passport bureau that issues a certificate by confirming the prospective signer identified in the certificate holds the corresponding private key. The requirement for CAs to establish proof of identity has led to the development of the Registration Authority (RA). RAs are responsible for the identification and authentication of certificate subjects, but do not sign or issue certificates. In some cases, the CA performs the subscriber registration function internally.

While digital signatures are generally the most certain method for assuring identity electronically, policy documents must identify how a signer’s identity is bound to their public key in a digital certificate – certificate policy statement. The strength of this binding depends on the assumption that only the owner has sole possession of the unique private key, and whether the private key is placed on a highly secure hardware token, such as a smart card.

The graphic below depicts the PKI process from the initial digital signature application process.

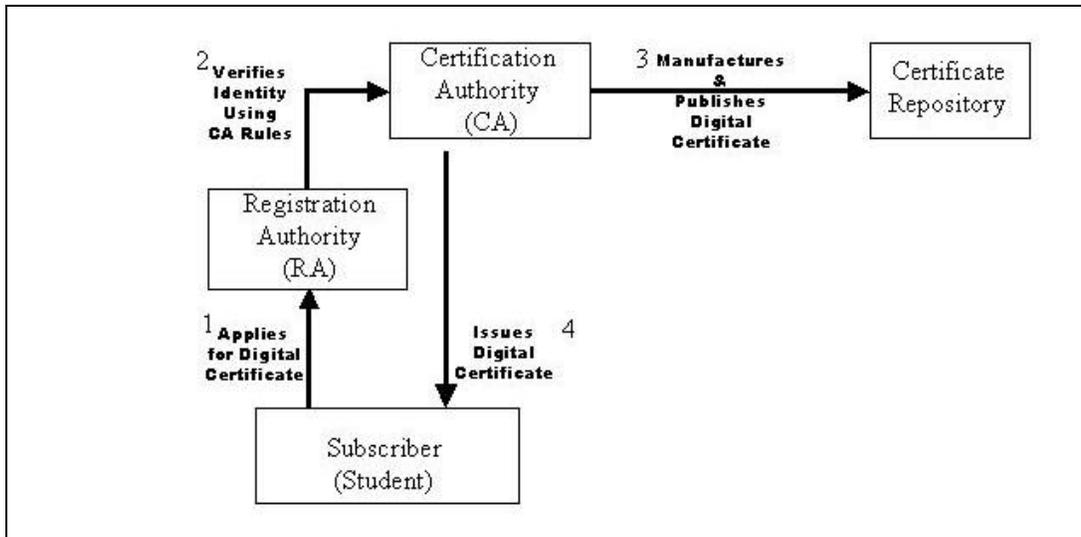


Figure 1 Subscriber Being Issued Digital Certificate

1. the Subscriber applies for a Digital Certificate from a Registration Authority (RA).
2. the RA must verify that the subscriber has proven their identity according to the rules established by the Certification Authority (CA).
3. the CA then creates and stores the new digital certificate to its Certificate Repository.
4. the CA issues the digital certificate to the subscriber.

The graphic below depicts the use of the Digital Certificate by a Subscriber.

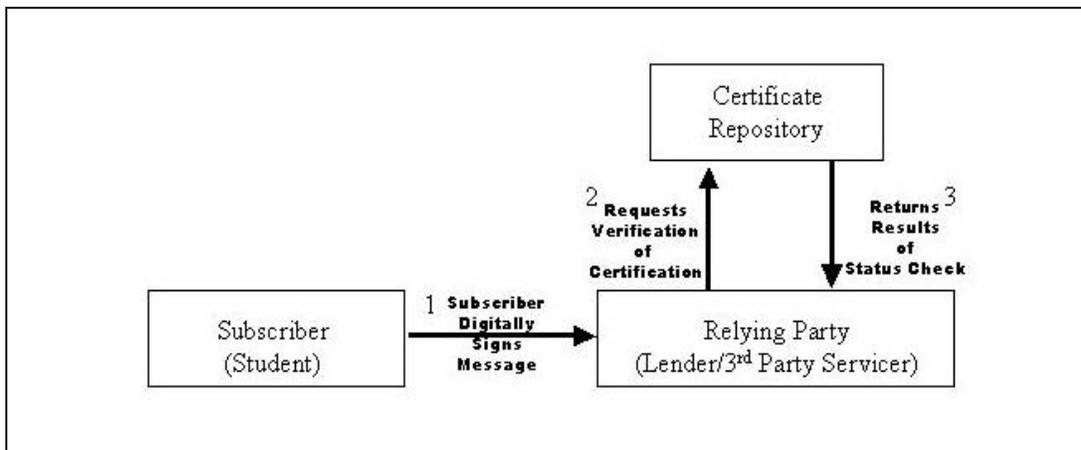


Figure 2 Subscriber Using Digital Certificate

1. The Subscriber presents their digital certificate to the Relying Party.
2. The Relying Party then checks the validity of the digital certificate with the CA against the CA's Certificate Repository.
3. The Certificate Repository returns a status result to the Relying Party.

5 WHY DIGITAL SIGNATURES?

With the forms of electronic authentication available today, what makes digital signatures a viable alternative to the wet signature? In order to understand the answer, we have considered the options in the table below.

Comparison of E-Signature Options

Requirement	Current Paper Based System	Proposed PIN Based System	Proposed Personal Uniform Resource Locator (URL) Based System	Proposed USPS Digital Signature Based System
Identify Proofing	High Signed Master Promissory Note	Medium Signed FAFSA (with SSA verification)	Medium Signed FAFSA (with SSA verification)	High Signed Disclosure and Proof of Identity to USPS
Infrastructure Development	Low Imaging	Medium PIN Database Database Infrastructure Archiving/Retrieval system	High Web page space for each user Web infrastructure Communications Infrastructure PIN Database Database Infrastructure Archiving/Retrieval system	Low Lender – Web based application USPS – Certificate processing infrastructure ED – Disclosure, documentation infrastructure All – Archiving/Retrieval system
Infrastructure Maintenance	Low	Medium Must maintain the PIN database	High Must maintain the PIN and the URL databases	Low
Adaptability to Internal Business	Easy	Easy	Easy	Easy
Adaptability to External Business	Easy	Difficult PIN database is a closed system	Difficult PIN / URL database is a closed system	Easy
Fraud Enforcement Responsibilities	Singular ED	Singular ED	Singular ED	Multiple USPS, ED, Third-Parties

Given the stronger identify proofing requirements, the multiple external business opportunities and the higher fraud enforcement, digital signatures are a clearer choice when considering e-signature alternatives.

5.1 Writing and Signature Requirements⁷

Signature requirements are, in essence, formalities. In many cases applicable statutes and regulations require that an agreement be both (1) documented in "writing" and (2) "signed" by the person who is sought to be held bound in

⁷ American Bar Association, Digital Signature Guidelines Tutorial, July 2000.

order for that agreement to be enforceable⁸. The FFEL process is no different. Before a loan agreement is finalized the lender must have a signed copy of the student's master promissory note.

Signing writings serve the following purposes: authenticity, data integrity, non-repudiation, and confidentiality. A signature authenticates a writing and attributes the signed document to the owner of the signature – authenticity. A signature on a document imparts a sense of clarity and completeness to the transaction – data integrity. In certain instances, a signature means the signer's approval or authorization of the document – non-repudiation. And finally a signed document transfers intent.

5.2 Digital Signature Standards

For electronic signatures to be viable, from both a legal and business perspective, the electronic signatures that are exchanged between signer and content originator must meet the same standards as the wet signature: authenticity, data integrity, non-repudiation, and confidentiality.

GPEA defines "electronic signature" as follows: "... a method of signing an electronic message that – (A) identifies and authenticates a particular person as the source of the electronic message; and (B) indicates such person's approval of the information contained in the electronic message."⁹

Authentication, data integrity, non-repudiation and confidentiality are the core security services provided by a PKI. These services enable entities to prove that they are who they claim to be, to be assured that important data has not been altered in any way, and to be convinced that data sent to another entity can be read only by that entity. Organizations can derive tremendous benefits from these services by using them to ensure, for example, that highly sensitive information only gets into the hands of those with an explicit "need-to-know."¹⁰

5.2.1 Authenticity

Authenticity refers to the process of ensuring that transmissions and messages, and their originators, are authentic, and that a recipient is eligible to receive specific categories of information.¹ Authentication validates the identity of parties in communications and transactions. Authenticity is concerned with the source or origin of a communication. Who is the message from? Is it genuine or a forgery? A party entering into an online contract must be confident of the authenticity of the communications it receives.

5.2.2 Data Integrity

Data integrity relates to the accuracy and completeness of the communication. The receiver must be able to ensure that the source data has not been accidentally or maliciously altered. Is the document the recipient received the same as the document the sender sent? Is it complete? The recipient of an electronic message needs to be confident of a communication's integrity before they will rely and act on it.

5.2.3 Non-repudiation

Non-repudiation is concerned with holding the sender to his communication. The sender should not be able to deny having sent the communication if he did, in fact, send it, or claim that the contents of the communication as received are not the same as what the sender sent if, in fact, they are what was sent. Non-repudiation is essential to electronic transactions when it comes to a relying party's (i.e. lender, ED, federal judge) willingness to rely on a communication, electronic contract, or funds transfer request.

⁸ American Bankers Association, Certification Authority Liability Analysis, February 1998

⁹GPEA, section 1709(1).

¹⁰ Carlisle Adams and Steve Lloyd, Understanding Public Key Infrastructure, MacMillan Technical Publishing

5.2.4 Confidentiality

Confidentiality refers to the process of ensuring that information can be read only by authorized entities. Digitally signed documents will remain confidential between the sender and receiver. However, digitally signed confidentiality is limited to two variables, 1) who has the signers public key and 2) has another entity been able to maliciously capture the signers transmission.

How signature requirements are met

Signature Requirements	Wet Signature	ED PIN/URL	Digital Signature
Authenticity	Signature is matched to the owner and attached to the document.	PIN, SSN, and Date of Birth are matched to owner.	The public key is matched to the owner and attached to the document which is used to read the contents.
Data Integrity	Imparts clarity and completeness.	Session is conducted through SSL and considered secure.	Association of document contents with the digital signature imparts completeness.
Non-repudiation	Signals approval and authorization.	Only owner knows PIN/URL.	Only the holder of the private key can create a digital signature and message that can be read with holder's public key.
Confidentiality	Transfers clarity and completeness to authorized readers.	Session is conducted through SSL and no other users are given access to personal web pages.	Document contents and public key can remain confidential between sender and receiver. Document and public key can be transferred by owner as necessary.

5.3 Supporting Digital Signatures with Public Key Infrastructure

For electronic communications, digital signature technology coupled with the Public Key Infrastructure (PKI) offers information security measures available to satisfy the business requirements of wet signatures: authenticity, data integrity, non-repudiation, and confidentiality.

5.3.1 Providing Authenticity

In public key cryptography, each user generates an encryption key pair consisting of two very long numbers known as keys. These keys have a special mathematical relationship in that any message encoded with one key can only be decoded with the other key. All keys and key pairs are unique – no two keys are identical. Before a sender can digitally sign an electronic communication, the sender must first generate a key pair using appropriate software. One of the keys is designated as the "private key" and the other key is designated as the "public key." A unique key pair being matched to one person forms authenticity.

5.3.2 Providing Confidentiality

The private key is kept confidential by the sender, and is used for the purpose of creating digital signatures. The public key can be disclosed generally by posting the key in online databases, repositories, or anywhere else the recipient of the digitally signed message can access it.

5.3.3 Providing Non-repudiation

To digitally sign an electronic communication, the sender runs a computer program that creates a unique message digest (or hash value) of the communication. The program then encrypts the resulting message digest using the sender's private key. The encrypted message digest is the digital signature. The sender then attaches the digital signature to the communication and sends both to the intended recipient. The attached digital signature proves the sender sent their communication – the sender cannot deny the digital signature.

5.3.4 Providing Data Integrity

When a recipient gets a digitally signed communication, the recipient's computer runs a computer program containing the same cryptographic algorithm and hash function the sender used to create the digital signature. The program automatically decrypts the digital signature (the encrypted message digest) using the sender's public key. If the program is able to decrypt the digital signature, the recipient knows that the communication came from the purported sender, that is, the recipient has verified its authenticity. This is because only the sender's public key will decrypt a digital signature encrypted with the sender's private key.

The program then creates a second message digest of the communication and compares the decrypted message digest with the digest the recipient created. If the two message digests match, the recipient knows that the communication has not been altered or tampered with, that is, the recipient has verified its integrity.

6 CURRENT FFELP LOAN REQUIREMENTS AND BUSINESS PROCESSES

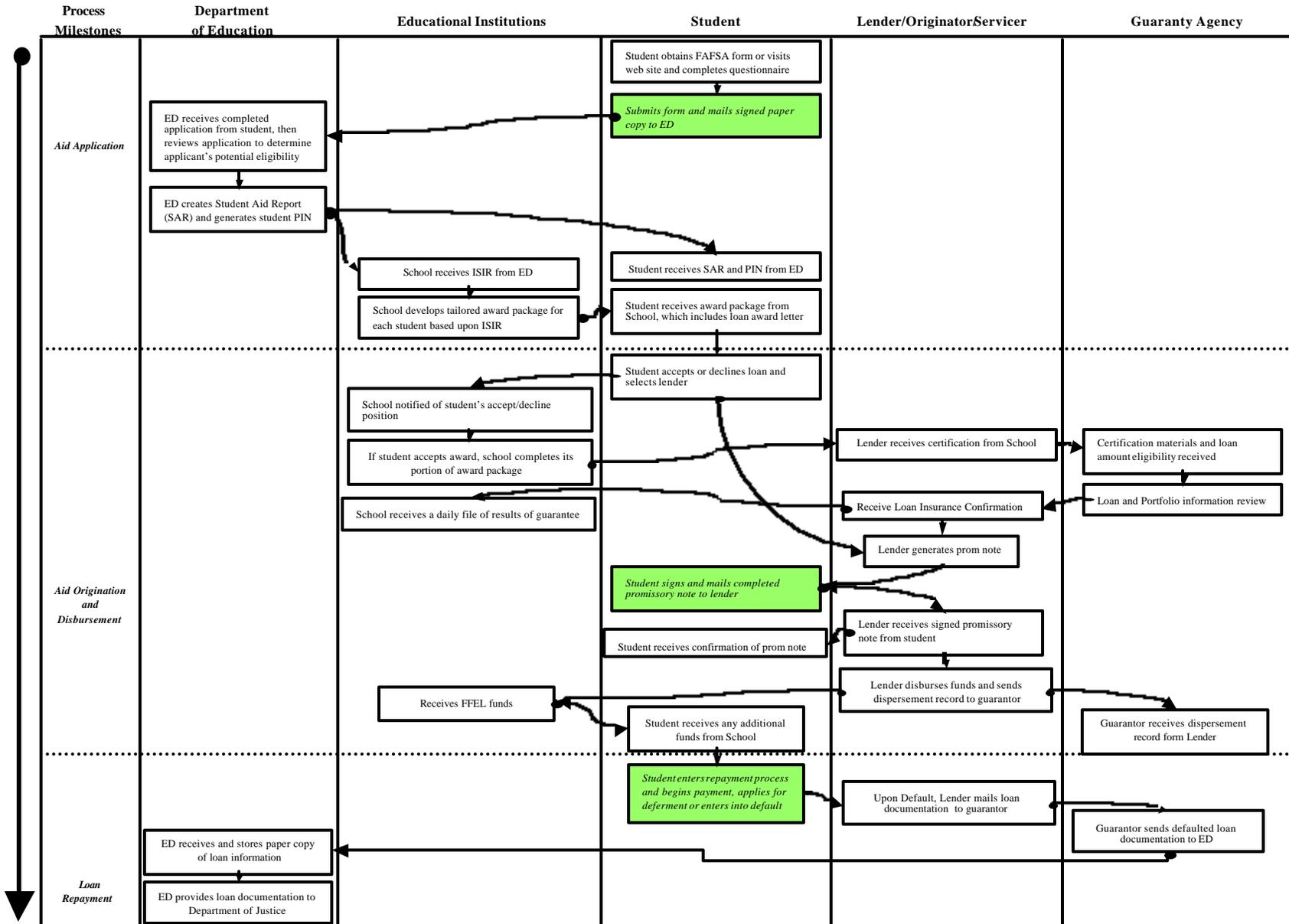
The FFEL Program has evolved from a purely paper-based process to a process that has eliminated the majority of its paper output in favor of leveraging the Internet to decrease costs and increase efficiency. Currently, the FFELP requires paper to be exchanged only for the signature of the FAFSA, the signature of the MPN, and the documentation of servicing due diligence.

The flow chart below, categorized by constituency and employing the SFA Modification Plan guidance, portrays the FFELP process as it currently exists in a simplified form.¹¹ The purpose of the chart is to create a flow chart of the current process and to identify specific points in the process where a signature is required to complete the necessary transaction.

¹¹ Appendix B contains a written description of the current process that further describes the roles and responsibilities of each constituent.

Signature needed

Current FFELP Prom Note Process



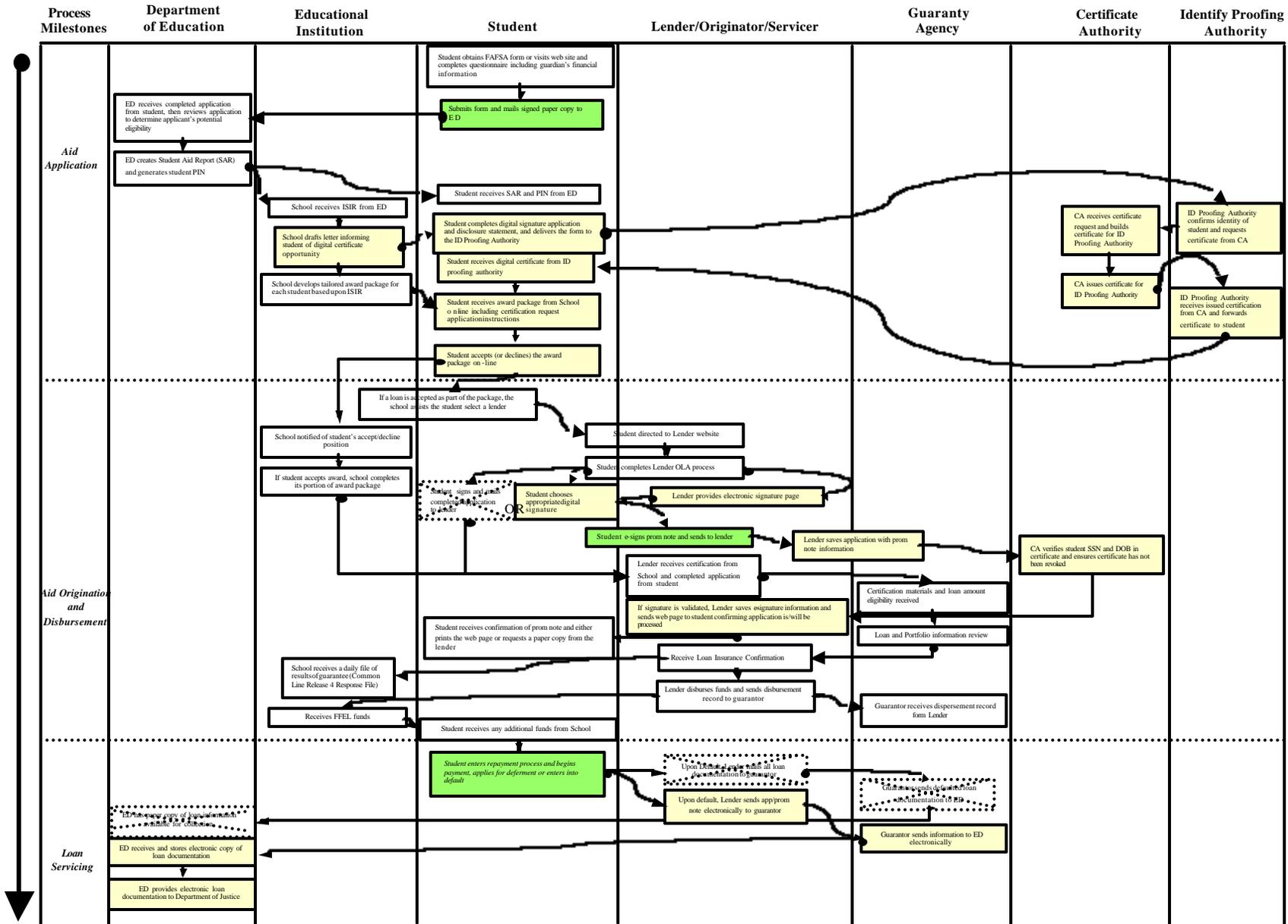
7 FFELP LOAN REQUIREMENTS AND BUSINESS PROCESSES USING DIGITAL CERTIFICATES

Achieving a completely electronic loan process would be in the interest of all FFEL partners. The efficiencies and cost savings that result from a paperless loan process will benefit the student, the school, the lender, and the Department. In order to achieve this objective, there needs to be an acceptance of PKI, digital signatures and their enforceability in a court of law.

Transferring from the current loan process to a PKI method of signing specific loan documents potentially could prove too burdensome for the student to adopt. To alleviate this burden, the Department could create a process that does not significantly burden any one constituency to an unnecessary degree. In the sections below, this paper describes a modified process that takes into consideration the burdens of each constituent, the costs involved, and the benefits of proceeding with this model. The process flow below depicts the modified FFELP promissory note process using digital signatures.

Signature needed

Modified FFELP Prom Note Process Using Digital Signatures



7.1 Student

In changing to a PKI model, the student should obtain a digital certificate early in the loan application process. To acquire the digital certificate, the school should inform the student they can apply for a digital certificate. Upon receiving a letter about the digital certificate process, the student could complete a digital certificate application and deliver the completed form to an identity proofing authority. After completion of the ID proofing process, the student could then receive the digital certificate in the mail or through a browser download.

Once the student accepts all or a portion of the award package delivered by the school, the student could be directed to a lender's web site. Rather than signing and mailing paper MPN, the student could utilize the digital signature to complete an electronic MPN form. Then a student could receive an electronic confirmation from the lender that the promissory note was received and accepted.

7.2 Educational Institution

The educational institution could perform one task beyond what they currently do. At some point during the aid application process, the school could inform the student of the digital signature opportunity. The school could send a letter informing the student of not only the process by which he/she could obtain the certificate, but also of the benefits accompanying the use of digital signature technology. Whether these benefits include monetary incentives, integrated capabilities within their campus, or some other unforeseen future benefit, the institution could explain to the student on the potential benefits of a digital certificate in this informational letter.

7.3 Lender and Guarantor

A PKI model may place new requirements on a lender/originator and may necessitate a solid investment by the lender. Many lenders already service the student through a web session, but cannot complete the loan application process without a wet signature. A totally electronic process could eliminate this burden by allowing the student to use their previously obtained digital signature to complete the loan application. By allowing the promissory note to be signed with a digital signature, the lender forgoes the burden of processing the mailed paper copy. Another potential requirement for a lender would be to establish a relationship with a certification authority (CA). This would be needed to allow the lender to confirm the student's identity, and permits the lender to accept the student's digital signature.

The benefits for the lender/originator are numerous and continue throughout the aid origination and disbursement process into the loan repayment process. If a student enters into default, the lender currently has to process a large quantity of paper records and mail those records to the guaranty agency. In a totally electronic PKI process, these transactions occur electronically. The potential savings in time and money realized by this modification should be substantial. The savings for the guaranty agency also should be substantial and similar to the savings experienced by lenders. Any time a process can be automated and paper eliminated, increased savings should be realized over time.

7.4 Department of Education

Under a totally electronic PKI process, the Department should change one portion of its current process: how it stores data. The Department should maintain a student's promissory note information electronically, as opposed to paper, for defaulted loans. Beyond this modification, the Department is not required to alter its business process. The Department should, however, remain vigilant in its oversight and monitoring of the loan process from its origination to its completion. This aspect does not diminish, but rather increases with the incorporation of digital signatures into the FFEL Program.

7.5 Certification Authority and Identification Proofing Authority

The CA and Identity Proofing Authority, two new entities in the modified process, work closely together during the initial aid application process. Upon receiving the information letter from the educational institution, the student completes the digital signature application and presents the application and personal identification materials to the identity proofing authority. Once the identity of the student is confirmed, a certificate is requested from the CA. The CA builds the certificate, issues the certificate and delivers the certificate to the identity proofing authority. This process can occur within seconds if a public/private key exchange is the preferred method to transmit the student's digital signature. However, the CA and identity proofing authority may choose to use certified mail to deliver the certificate.

The CA enters the business process again when the lender requires the student's digital certificate to be verified. The CA verifies the student's social security number and date of birth, as well as ensures that the certificate being used by the student to sign the promissory note has not been revoked. The continued responsibility of the CA is to maintain the certificate in a secure environment until the loan expires or the student no longer needs the digital signature.

8 DIGITAL SIGNATURE OPTIONS

PKI is an open standards theory that enables entities, both individuals and organizations, to identify themselves to their customers and clients with the guarantee of a third party not materially involved in the transaction. Numerous publications and standards from the National Institute of Standards (NIST) are available for guidance in the implementation of PKI. All PKI implementations need to conform to a minimum set of technical standards issued by NIST. It is the additional features that are needed for a particular implementation that differentiates the PKI, such as identity proofing and key recovery. The publications and standards relevant to PKI are indicated below:

- FIPS PUB 186-2 *Digital Signature Standard*
- FIPS PUB 180-1 *Secure Hash Standard*
- FIPS PUB 171, *Key Management using ANSI X9.17*
- FIPS PUB 140-1, *Security Requirements for Cryptographic Modules*
- FIPS PUB 73, *Guidelines for Security of Computer Application*
- FIPS PUB 46-3, *Data Encryption Standard*
- ANSI X9.31-1998, *Digital Signatures Using Reversible Key Cryptography for the Financial Services Industry*
- ANSI X9.62-1998, *Public Key Cryptography for the Financial Services Industry*

8.1 Operational Considerations

By implementing the above-mentioned standards into a major application as defined in the OMB A-130, any entity has the ability to provide the baseline services of a certificate authority. These minimum services are issuance, revocation, and validation and are provided by all of the PKI vendors included in this analysis.

What sets each vendor apart is the additional services that are provided to the customers. When choosing a vendor for a PKI implementation, it is important that the decision is based upon the additional services that are required, not just available. Examples of additional services include strong identity proofing, key recovery, and certificate customization.

8.1.1 Web browser vs. Smart Card

Digital certificates are capable of being stored on either an external device such as a smart card or floppy disk, or they can be embedded within an application such as a web browser. For security reasons the optimal implementation would use an external device that stores the digital certificate in an encrypted form accessible via a secret pin. However for the pilot, cost, availability, and time to market must be taken into consideration. For this reason we have chosen the web browser implementation of digital certificate storage.

For the digital certificate pilot, it is possible that if an individual uses a publicly shared computer and does not remove their digital certificate from the web browser, another individual could use the same publicly shared computer and access the previous user's private key.

8.1.2 Identity Proofing

For identity proofing, proper procedures must be implemented to verify the identification of an individual prior to issuance of a digital certificate. These procedures should vary with the level of privilege that is being requested by that individual. In the current student aid model, students are required to show some form of identification. This procedure should be continued into the electronic-based FFELP so that there are no new legal issues that would have to be addressed. Each possible PKI vendor's implementation has their own method of proofing and each vendor's implementation has to be judged at how their proofing service meets SFA's requirements.

8.1.3 Storage of Digital Signature Results (eNote)

In order to consider an optimal way of storing the eNote, numerous issues must be addressed. Identification of signer, change in loan servicing company, and loan enforcement provisions must be taken into account. SFA should develop and support an open standard that will be used by all partners in the student aid processes. An option that should be further explored is the use of eXtensible Markup Language (XML), XML is the new open standard. Numerous consortiums exist within the industry whose sole purpose is to publish interoperability standards. Several banking institutions have integrated XML into loan applications however there is yet to be any standard regarding XML and loans.

8.1.4 Lookups – One Time vs. Many

When considering a PKI-based implementation, policies and procedures will effect operations and the cost of the implementation. In the current paper-based operation, a signature is never notarized but rather the individual is identified before signing the loan. If SFA moves to an electronic-based signature, it would be possible to either verify the digital signature on the loan at origination or verify at every stage of the electronic document's life.

8.2 Operational Alternatives

The proceeding analysis will analyze three PKI operational alternatives. The analysis will utilize consistent criteria to objectively determine the most appropriate product to be used in the FFELP pilot project.

8.2.1 Verisign

The most widely known implementation of public key infrastructure is from Verisign, Inc. of Mountain View, California. They have solutions available for trust services, web sites, developers, and individuals. Their product called OnSite enables entities to set up their own RA and manage certificates using Verisign's infrastructure. The customer's administrator is given a smart card, which is used in the identification and authentication of administrator authority. The administrator authority has the ability to issue, deny, and revoke certificates.

Individuals who apply for a certificate go to a web site hosted by Verisign and configured by the administrator. The individuals provide all of the required information including one additional field called the pass-phrase. This field is not in the X.509V3 certificate, but rather is used for administration purposes. This field is used as a "proofing" mechanism where the individual must know the pass-phrase the administrator is expecting.

A distinguished difference in the Verisign product is its "Key Recovery" capability. A server is configured at the customer site, which contains the private key of all users in encrypted form. If for any reason a user needs to recover their private key, Verisign will use the server at the customer site and provide a unique recovery key to the individual's private key. At that point the users private key would become available to the user.

In the charts below, low represents – an automated process, medium - a pass-phrase response to an automated process, and high – an in-person proofing process.

The prices below are the non-negotiated annual prices from the Verisign web site for issuance, lookup, and the administrator's kit.

8.2.2 ACES

Access Certificates for Electronic Services (ACES) is a government program sponsored by the General Services Administration (GSA) that provides a framework for agencies moving into the PKI arena. This framework enable agencies to procure PKI services from corporations and other executive branch agencies by providing a standard list of contractual deliverables and milestones. Under this program, agencies are charged for the hours of service in a particular labor category as well as a certificate validation fee.

This customizable solution enables agencies to implement a PKI solution that is specifically tailored to the agencies needs. For example, AT&T's ACES implementation uses Verisign services on the back end, but AT&T employees for product customization.

8.2.3 USPS

Under the United States Postal Services (USPS) implementation, individuals who need a certificate go to their local post office and present proof of identity. The postal employee verifies the identify of the individual and transmits the certificate application to the certificate processing center. At the certificate center the individual's public and private key is generated, written to a media (floppy, smart card, token), and mailed to the individual at the address listed on the application.

The USPS pilot project implementation currently will issue the public and private keys on a floppy disk. The cost for this pilot project is 50 cents for each certificate issuance and 40 cents for each lookup. The specific monetary discussion provided here are initial estimates that were provided in meetings with USPS. No existing documentation on pricing is available for consideration.

8.3 Summary

In all of the above implementations, fundamental PKI services provided by the vendors are the same. Each vendor provides the services for the issuance, revocation, and validation of digital certificates using known standards. However, each vendor provides additional services which differentiate themselves from their competitors. The table below lists the different implementations by vendor and their distinguishing characteristics.

In the tables below we assume 5,000 certificates will be issued in a year. Verisign certificates expire after one year and must be renewed annually. The ACES model uses a contract vehicle which entails negotiations with a vendor for the services of configuring a registration authority as well as a per lookup/validation cost and expiration date. The USPS certificates validity periods would be configured to support the requirements of the FFELP process.

8.3.1 Feature Comparison

PKI Implementation	Type of Identity Proofing Available	Key Recovery Support	Online Certificate Status Protocol Support*
Verisign	Password	Yes	Current
ACES	Custom	Custom	Custom
USPS	In Person	Yes	Future

*Online Certificate Status Protocol (OCSP) Support allows entities to validate a client's digital certificate credentials in real-time (as the transactions occurs).

8.3.2 Cost Comparison

Issuing 5,000 digital certificates

PKI Implementation	Cost Per Certificate Issued	Total Cost of Issuance	Who Pays?
Verisign	\$14.59	\$72,950.00	Student
ACES	\$0.00	\$0.00	GSA*
USPS	\$0.50	\$2,500.00	USPS**

*GSA has set aside first 500,000 certificates at no cost.

**USPS has agreed to fund initial pilot.

Assuming 6,000 transactions

PKI Implementation	Cost per Transaction	Total Transaction Cost	Who Pays?
Verisign	\$0.00	\$0.00	Relying Party
ACES	\$0.85	\$5,100.00	ED*
USPS	\$0.40	\$2,400.00	Relying Party

*ACES is a Public-to-Government certificate program that has no mechanism for charging fees to a commercial entity, i.e. non-government relying party.

8.3.3 Differentiation

Vendor	Differentiation
Verisign	Industry leader with private key recovery
ACES	Allows for rapid contractual award given a specific PKI framework
USPS	Allows for strong proofing and protections of postal fraud laws and regulations

8.3.4 Recommendation

Based upon the features, costs and differentiators, the USPS meets or exceeds all of the requirements for a FFELP eSignature electronic MPN process.

9 RISKS, ISSUES AND CONCERNS

Assessing the implementation of PKI in the FFELP process involves a risk-analysis. OMB acknowledges neither handwritten signatures nor electronic signatures are totally reliable and secure. Every method of signature can be compromised with enough skill and resources, or due to poor security procedures, practices, or implementation. The risks of PKI to all entities involved in the FFELP process must be fully considered before they can be mitigated.

9.1 PKI Risk Categories

A signature of any type gives confidentiality, authentication, integrity and non-repudiation to an agreement or contract. A PKI digital signature also serves these functions, and as with a wet signature, has inherent risks. The risks to these signature functions when using PKI are detailed below.

Confidentiality. PKI without encryption of the message content allows anyone who receives or obtains the message to read it whether or not they were meant to see the message content. Confidentiality is at great risk without message content encryption should the sender mistakenly send the message to an unintended recipient, a malefactor intercepts the message, or the intended recipient passes the message on to someone who wasn't meant to see its contents. Information protected under the Privacy Act could be disclosed to those without a need to know.

Authentication. Should a signer's private key be stolen, the authenticity of the signature comes into question. Whoever acquires a private key that isn't their own could forge a digital signature, and the recipient can't be sure who the message is from, especially if the sender doesn't know his/her private key was stolen. Authenticity under PKI can also come into question if the registration authority conducts a weak proofing process.

Integrity. A document could be accidentally or maliciously altered between the time it leaves the sender and reaches the recipient. The document's contents could be changed or it could arrive incomplete. Depending upon the PKI application used, the recipient could be warned that the document isn't an exact match to what the sender sent when the document is opened.

Non-Repudiation. The signer and recipient can't disclaim the communication or transaction they made using PKI unless the signer's private key has been stolen. When a private key is stolen PKI can't support non-repudiation if the key thief forges communications.

9.2 PKI Issues and Concerns

Issue	Frequently Asked Question	USPS Digital Certificate (Dig Cert)	Recommendation	Status
Legality	<p>Is a digitally signed MPN legally binding?</p> <p>What are the legal requirements for an eSignature?</p> <p>What does an eMPN look like?</p> <p>How are digital certificates used in a court of law as evidence?</p> <p>What is everyone's liability in an electronic PKI environment?</p>	<p>Certificate binds identity to digital signature.</p>	<p>Legal enforceability remains an issue. Recommend that ED General Counsel be asked to provide guidelines for electronic identification and signature.</p>	<p>ED Legal/Policy is reviewing.</p>
Privacy	<p>How will system ensure Student's privacy will be protected?</p> <p>Is there an adequate "level of protection" for student users?</p> <p>Who will be responsible for tracking identity theft?</p>	<p>Dig Cert known to Certification Authority (USPS) & those who Student sends Dig Cert</p> <p>USPS Postal Inspectors ED DOJ</p>	<p>Ensure that disclosure statement clearly explains student responsibility for protection</p> <p>CIO Legal/Policy</p>	<p>All possible measures should be taken to ensure Student's privacy</p> <p>Possible need for a written Memorandum of Understanding outlining responsibilities with USPS</p>

Issue	Frequently Asked Question	USPS Digital Certificate (Dig Cert)	Recommendation	Status
Technology	<p>How will Browser based solutions be tailored to prevent eavesdropping?</p> <p>How can certificate be supported over a 30 year life of a student loan?</p> <p>How can a cert be used to tie data between a school/originator/lender and student?</p>	<p>Alternatives:</p> <ul style="list-style-type: none"> • Browser Based Dig Cert for MPN Use Only • Smart Card with Dig Cert • Diskette with Dig Cert 	Issue diskette with browser based certificate	Digital Certificate technology can support either alternative
Identify Proofing	What level of identify proofing is required?	<p>Two Options:</p> <ul style="list-style-type: none"> • No physical identity check – real time check against SSA • Physical identity check performed by USPS 	Physical identity check performed by USPS	Need written Legal/Policy statement of SFA Identity Proofing Standards
Operations	<p>What should be transferred from lender to guarantor to ED and how?</p> <p>How is revocation handled? Does a school revoke?</p> <p>What are start-up and on-going costs?</p>	Electronic record	CA will store the record	Need written Legal/Policy statement of SFA Identity Proofing Standards

Business Process – Loan Default

Issue	Frequently Asked Question	USPS Digital Certificate (Dig Cert)	Recommendation	Status
Loan Default	What are the minimum evidence/documentary requirements?	DOJ will not go to court without “true and exact” copy of MPN	Need written Legal/Policy review of documentation standards.	In process
Retrievability	What happens if the electronic eNote cannot be provided?		Need case-by-case analysis of each proposal to see how retrievability is addressed. ED Legal/Policy needs to coordinate with DOJ a resolution to this issue.	In process Pilot will help test alternative solutions.
Prevention of “Digital Rot”	Who would be liable if record could not be electronically produced?	USPS Guarantor Owner of Debt ED	Need case-by-case analysis of each proposal to see how “digital rot” is addressed. Possible Memorandum of Understanding outlining responsibilities for USPS.	In process Pilot will help test alternative solutions.
Transferability	When loans are sold what electronic records must transfer?	Digitally Signed Document Original Document	Need written guidance on electronic document standards	In process Pilot will help test alternative solutions.

Other

Issue	Concern	USPS Digital Certificate (Dig Cert)	Recommendation	Status
Acceptance	Will students use an electronic process?	Examine “take” rates during a pilot. Administer surveys to all in a pilot.	Examine “take” rates prior to going live Administer surveys to all in the pilot	CIO/Innovations develop survey plan prior to initiation of pilot. Evaluation of surveys will help determine alternative solutions.
Loss	What if student loses the certificate?	Certificate must be revoked.	Develop revocation and re-issue procedures	Pilot will help test alternative solutions.
Total Uncollectability	What happens to the eNote MPN if pilot fails?	Identity is established	A contingency plan must be developed prior to fielding pilot	Pilot will help test alternative solutions.
On-going Concern	What happens if the CA goes out of business or stops issuing digital certificates?	Not likely	A contingency plan must be developed prior to fielding pilot	Pilot will help test alternative solutions.

9.3 PKI Risks by Constituencies

The following table illustrates how the risks associated with PKI affect the FFELP constituencies.

	Confidentiality	Authentication	Integrity	Non-Repudiation
Student	<ul style="list-style-type: none"> • Private information like personal income and SSN revealed 	<ul style="list-style-type: none"> • Someone impersonates student and obtains digital certificate • Private key stolen and loan information forged 	<ul style="list-style-type: none"> • Digital certificate application altered during transmission between student and CA • Promissory note altered during transmission between student and lender 	<ul style="list-style-type: none"> • Thief steals student's private key and forges loan documents
School	<ul style="list-style-type: none"> • None identified 	<ul style="list-style-type: none"> • Issue - student login from school session to lender session 	<ul style="list-style-type: none"> • None identified 	<ul style="list-style-type: none"> • None identified
Lender/ Guarantor	<ul style="list-style-type: none"> • Release of private lender or student information 	<ul style="list-style-type: none"> • Lender accepts invalid student digital certificate • Lender can't verify student's digital certificate with CA 	<ul style="list-style-type: none"> • Promissory note altered during transmission between student and lender • Web session spoofed 	<ul style="list-style-type: none"> • Lender can't provide guarantor with electronic records of defaulted loans • Guarantor can't provide to the Dept of ED the electronically-stored student loan information for defaulted loans
Department of Education	<ul style="list-style-type: none"> • Information intercepted when forwarded to guarantor 	<ul style="list-style-type: none"> • None identified 	<ul style="list-style-type: none"> • Defaulted loan files altered during transmission to guarantor 	<ul style="list-style-type: none"> • Can't prove student signed promissory note • Can't retrieve electronically stored student data

	Confidentiality	Authentication	Integrity	Non-Repudiation
Certificate Authority and Proofing Authority	<ul style="list-style-type: none"> • None identified 	<ul style="list-style-type: none"> • Root CA compromised and fake certificates are issued • Lost or stolen certificates aren't reported and CA can't invalidate certificate before it's used to forge loan information • Student uses fake identification materials and proofing fails to stop student from applying for digital signature • Digital certificate doesn't make it to the student 	<ul style="list-style-type: none"> • Digital certificate altered during transmission from CA to student 	<ul style="list-style-type: none"> • None identified

10 NEXT STEPS

SFA needs to take steps to be better poised to make the transformation into an electronic environment. The legislative foundation is established and effective dates have been defined. The necessary technological capabilities are available. However, SFA may not be ready to move to a digitally signed MPN due to the following concerns:

- the lack of an identity proofing standard (E-Identification)
- digital signatures legal enforceability case law
- a clear mechanical understanding of PKI in the FFELP process

Given the current environment and benefits discussed throughout this white paper we recommend the following next steps:

- Review current regulations and determine if regulatory changes or supplemental guidance is needed
- Issue a FFELP “Dear Partner” Letter outlining SFA’s current position, desire to do a digital signature pilot, and ask for pilot proposals
- Move forward with a pilot

10.1 Review of Regulatory and Policy Parameters

There are Legal issues which require legal or policy guidance before implementation of a digital signature pilot:

1. Identify proofing standards in the digital certificate application process
2. Electronic documentation of loan evidence

The Policy issues surrounding the use of a digital signature pilot should be addressed in a Dear Partner letter giving a general opinion on the following topics:

1. Paper based prom notes for MPN is all that ED can support for now
2. Standards on level of proofing and use of electronic prom note for evidence in default cases are being developed and will be issued by July 2001, based on OMB guidance
3. ED will continue to work with the student aid industry as these standards are developed
4. ED will be working with pilots and possibly granting experimental site status to schools and offering a waiver of regulations for lenders.

10.2 Inform FFELP Partners

A “Dear Partner” letter should be drafted that informs our FFELP partners of SFA’s support for electronic signatures, states SFA’s intent to development regulatory and policy parameters for implementation of electronic signatures and suggests the possibility for FFELP digital signature pilot opportunities.

10.3 FFELP Digital Signature eMPN Pilot

Prior to the implementation of a PKI/digital signature pilot SFA would be required to review the proposed pilot to ensure that resulting electronic MPN would be enforceable. In order to facilitate the review and approval process, a business case will be developed that creates an evaluation matrix to analyze and prioritize potential pilot proposals, outlines a process for internal and external discussions, evaluates and selects proposals, and continues this process through pilot implementation.

Appendix A – Review of Recent Legislation

Recent legislation, the Government Paperwork Elimination Act and the Electronic Signatures in Global and National Commerce Act, reflects the Federal government's movement toward an electronic operating environment. According to the Office of Management and Budget, Federal agencies have until October 2003 to provide customers and users the option, when practicable, to electronically submit information or electronically transact with agencies. Agencies must be capable of using electronic signatures and accept them as valid, when practicable. The newest of the e-related legislation expands the use of electronic signatures from Federal operations into national and international commerce, eliminating the need for contracts and other records to be written and signed on paper. The Federal government has made an electronic signature the legal equivalent of a handwritten signature for government and commercial transactions, mandating its use by Federal agencies in the near future.

The proceeding section will provide a concise description of the Government Paperwork Elimination Act (GPEA), the OMB Procedures and Guidance on Implementing the GPEA, and the new E-signature act. The purpose of these sections is to provide the legislative context within which an evaluation of the digital certificate possibilities can occur.

Government Paperwork Elimination Act (GPEA)

The Government Paperwork Elimination Act (GPEA) of October 21, 1998 establishes the requirement for government agencies to provide for electronic submission, maintenance, or disclosure of information as a substitute for paper and for the use and acceptance of electronic signatures. The term "electronic signature" is defined to mean a method of signing an electronic message that identifies and authenticates a particular person as the source of the electronic message and indicates such person's approval of the information contained in the electronic message. GPEA requires agencies develop plans for "electronic government" by October 2000, achieving implementation by October 2003. In essence, GPEA provides legal recognition for electronic signatures made for the purpose of signing and filing electronic documents with Federal agencies.

Government Paperwork Elimination Act - Requires the Director of the Office of Management and Budget: (1) in providing direction and overseeing the acquisition and use of information technology, to include alternative information technologies that provide for electronic submission, maintenance, or disclosure of information as a substitute for paper and for the use and acceptance of electronic signatures; (2) to develop procedures for the use and acceptance of electronic signatures by executive agencies; (3) to ensure that, within five years, executive agencies provide for the option of electronic maintenance, submission, or disclosure of information as a substitute for paper and for the use and acceptance of electronic signatures, when practicable; (4) to develop procedures to permit private employers to store and file electronically with executive agencies forms containing information pertaining to employees; and (5) in cooperation with the National Telecommunications and Information Administration, to conduct and report the Congress on an ongoing study of the use of electronic signatures on paperwork reduction and electronic commerce, individual privacy, and the security and authenticity of transactions.

(Sec. 1707) Provides for: (1) the enforceability and legal effect of electronic signatures; (2) protection from disclosure of information collected in the provision of electronic signature services for executive agencies; and (3) applicability exceptions with respect to administration of the internal revenue laws.

OMB Procedures and Guidance on Implementing the GPEA

The OMB issued implementation instructions for GPEA on May 2, 2000. Rather than providing specific systems and technical guidelines, OMB sets forth general policies and procedures for implementing the Act, then offers Federal managers more practical implementation guidance. This guidance discusses risk assessment requirements, privacy and disclosure issues, current electronic transaction technologies, and the processes an agency should follow to evaluate electronic alternatives. Throughout the document, OMB refers to and recommends compliance with a number of existing policies to provide a broad, common framework for ensuring the implementation of electronic systems in a secure manner.

As agencies set out to enact the GPEA, their procedures should be executed with due consideration of the following policies:

1. maintaining compatibility with standards and technology for electronic signatures generally used in commerce and industry and by State governments;
2. not inappropriately favoring one industry or technology;
3. ensuring that electronic signatures are as reliable as appropriate for the purpose in question; maximizing the benefits and minimizing the risks and other costs;
4. protecting the privacy of transaction partners and third parties that have information contained in the transaction;
5. ensuring that agencies comply with their record keeping responsibilities under the FRA for these electronic records. Electronic record keeping systems reliably preserve the information submitted, as required by the Federal Records Act and implementing regulations; and
6. providing, wherever appropriate, for the electronic acknowledgment of electronic filings that are successfully submitted (OMB Guidance, Part I, Section 1)

OMB instructs agencies to conduct an assessment of whether to use and accept documents in electronic form and to engage in electronic transactions. The assessment should weigh costs and benefits and involve an appropriate risk analysis, recognizing that low-risk information processes may need only minimal consideration, while high-risk processes may need extensive analysis. The assessment should develop strategies to mitigate risks and maximize benefits in the context of available technologies. In addition to serving as a guide for selecting the most appropriate technologies, the assessment of costs and benefits should generate a business case and verifiable return on investment to support agency decisions regarding overall programmatic direction, investment decisions, and budgetary priorities. In doing so, agencies should consider the effects on the public, its needs, and its readiness to move to an electronic environment.

OMB's guidance describes the following non-cryptographic and cryptographic electronic signature alternatives that an agency could employ:

- Personal Identification Number (PIN) or password
- Secure Sockets Layer (SSL) with PIN or password
- Smart Card
- Digitized Signature
- Biometrics
- Shared Symmetric Key Cryptography
- Public/Private Key (Asymmetric) Cryptography – Digital Signatures (i.e., Public Key Infrastructure (PKI))

Electronic Signatures in Global and National Commerce Act

Signed into law in June 2000, this Act seeks to facilitate the use of electronic records and signatures in transactions affecting interstate or foreign commerce. The Act clarifies the legal validity of electronic contracts, signatures, notices, and other records, and allows contracting parties to choose the technology for authenticating their transactions without government intervention. The Act also will ensure on-line consumers will have legal protections equivalent to those in the off-line world. Consumers retain the choice to do business and receive records on paper or on-line. Like the above legislations, this Act maintains a technology neutral position for implementing electronic signatures. Some of the practical aspects of the Act are:

No Consumer Requirement to Use Electronic Records:

Section 101(b)(2) does not require any person to agree to use or accept electronic records or electronic signatures, other than a governmental agency with respect to a record other than a contract to which it is a party.

Affirmative Consent by the Consumer is Required:

Section 101(c)(1)(A) stipulates that the consumer must affirmatively consent to the use of an electronic record and has not withdrawn such consent. However, the legal effectiveness, validity, or enforceability of any contract executed by a consumer shall not be denied solely because of the failure to obtain electronic consent or confirmation of consent by that consumer, per Section 101(c)(3).

Informed Consent by the Consumer is Required:

Section 101(c)(1)(B) stipulates that the consumer, prior to consenting, must be provided with a clear and conspicuous statement informing the consumer of any right or option of the consumer to have the record provided or made available on paper or in nonelectronic form and the right of the consumer to withdraw the consent to have the record provided or made available in an electronic form and to update information needed to contact the consumer electronically.

Breadth of Consumer's Consent Must be Clear:

Informed consent also requires informing the consumer of whether the consent applies only to a particular transaction or to identified categories of records that may be provided or made available during the course of the parties' relationship.

Conditions and Consequences of Withdrawal of Consumer's Consent:

The consumer must also be informed of any conditions, consequences (which may include termination of the parties' relationship), or fees in the event of withdrawal of consent to use electronic records and describing the procedures the consumer must use to withdraw consent. If revised future hardware and software requirements limit the consumer's ability to use electronic records, the consumer has the right to withdraw consent for electronic records without the imposition of any fees for such withdrawal and without the imposition of any condition or consequence. Withdrawal of consent does not affect the legal validity of electronic records agreed to prior to withdrawal of consent.

Consumer Options for Requesting Paper Copies:

The consumer must be informed how, after the consent, the consumer may request a paper copy of an electronic record, and whether any fee will be charged for such copy.

Consumer Demonstration of Capability:

Prior to consenting to an electronic transaction, the consumer must be provided with a statement of the hardware and software requirements for access to and retention of the electronic records and consents electronically, or confirms his or her consent electronically in a manner that reasonably demonstrates that the consumer can access information in the electronic form that will be used to provide the information that is the subject of the consent.

Software and Hardware Upgrade Issues for Consumers:

If a change in the hardware or software requirements needed to access or retain electronic records creates a material risk that the consumer will not be able to access or retain a subsequent electronic record, the person providing the electronic record must provide the consumer with a statement of the revised hardware and software requirements and the right to withdraw consent for electronic records.

Verification or Acknowledgement of Records:

If a prior law expressly requires a record to be verified or acknowledged through a receipt, the record may be provided or made available electronically only if the method used provides verification or acknowledgment of receipt.

Electronic Oral Communications:

Oral communication or recording of such communications does not qualify as an electronic record for purposes of this Act unless otherwise provided by law.

Accessibility and Accuracy Over Time:

If a contract or other record of a transaction must be maintained pursuant to statute, regulation, or other rule of law, that requirement is met by retaining an electronic record that accurately reflects the information, remains accessible to all persons entitled to access, and can be accurately reproduced for later reference.

Notarization of Documents:

If notarization, acknowledgment, verification, or sworn statements under oath are required, an electronic signature will be valid if the person is authorized to perform those acts and if all other information required to be included by other applicable statutes is attached or logically associated with the electronic record.

Document Integrity When Third-Party e-Agents are Used:

A contract or other record relating to a transaction in or affecting interstate or foreign commerce may not be denied legal effect, validity, or enforceability solely because its formation, creation, or delivery involved the action of one or more electronic agents so long as the action of any such electronic agent is legally attributable to the person to be bound.

Impact of the Laws of the Individual States:

A State statute, regulation, or other rule of law under certain circumstances may modify, limit, or supersede the Act only if such statute, regulation, or rule of law constitutes an enactment or adoption of the Uniform Electronic Transactions Act as approved and recommended for enactment in all the States by the National Conference of Commissioners on Uniform State Laws in 1999.

Excepted Requirements for Specified Transactions:

As a generalization, the provisions of the Act are not intended to apply to wills, codicils, or testamentary trusts; govern adoption, divorce, or other matters of family law; the Uniform Commercial Code of any State; court orders or notices, the cancellation or termination of utility services; certain specified credit agreements or rental agreements secured by a primary residence; cancellation of certain types of insurance; product recalls; or handling or transportation of hazardous materials.

Standards for Accuracy, Integrity, and Accessibility:

A Federal regulatory agency or State regulatory agency may interpret the Act to specify performance standards to assure accuracy, record integrity, and accessibility of records that are required to be retained. Such performance standards may be specified in a manner that imposes a requirement in violation of certain provisions of the Act if the requirement serves an important governmental objective; and is substantially related to the achievement of that objective. In addition, under certain circumstances, a Federal regulatory agency or State regulatory agency may interpret the Act to require retention of a record in a tangible printed or paper form.

Software and Hardware Neutrality

Nothing in this paragraph shall be construed to grant any Federal regulatory agency or State regulatory agency authority to require use of a particular type of software or hardware.

Roles of the Department of Commerce, USPS, and FTC:

The Secretary of Commerce shall conduct an inquiry regarding the effectiveness of the delivery of electronic records to consumers compared with the delivery of written records via the United States Postal Service and private services. The Secretary shall also conduct a joint review of the process with the Federal Trade Commission for other purposes.

Transferable Records and Proof of Control:

The Act sets out requirements that must be met to demonstrate the conditions under which a person is deemed to have control of the authoritative electronic record and be authorized to transfer the control of that record to a third party.

Appendix B – Current FFELP Prom Note Process

Student

A student no longer is required to complete a FAFSA with pen and paper; rather, a student completes the FAFSA on-line. The on-line application process allows the student to electronically submit his/her application to the Department of Education. However, the student is required to print out the signature portion of the application, sign the form in the designated field, and mail the signed document to the Department.

The student's role in the loan process continues upon receipt of the Student Aid Report (including potential school contribution) from the school. This on-line process is completed upon the student's acceptance (or denial) of each line-item in the award package. Having selected each line-item in the award package, the student is directed to a lender's web site where he/she completes an on-line application. The last step in the on-line application process is to print out the signature page and mail the completed promissory note to the lender.

Once the lender has processed the student's promissory note, the student receives either an on-line verification or a paper copy from the lender. Upon completion of schooling, the student enters the repayment portion of the loan process. If the student defaults on the loan, the lender, guaranty agency and the Department of Education attempt to collect all outstanding funds from the student.

Educational Institution

The educational institution's role in the loan process is principally a support function. The school acts as a processor of information and a gateway of information between the Department of Education, the student and the lender. The most important roles the school performs are to deliver an award package to the student, receive the FFEL funds from the lender, and apply the funds to the appropriate student's account.

The burden placed on the educational institution is has been minimized by the lender and the Department of Education. After the student concludes his/her relationship with the school, the school may enter the repayment process if a student defaults in order to aid the collectors locate the delinquent borrower.

Lender and Guarantor

The lender enters the loan process when the student decides to accept the award package presented by the school. Generally, on the school's web site, the student follows a hyperlink button to one of the school's preferred lending institutions. At the lender's site, the student signs into a loan application session. The student sign-in triggers his/her authentication by transmitting the student's school identification number to the lender. The lender further authenticates the student by requiring him/her to enter a social security number and date of birth. The student completes the application on-line until he/she encounters the signature portion of the form. At this stage, the student prints, signs and mails the promissory note to the lender.

Upon receipt of the student's signed application and the file/paper from the school, the lender delivers the certification materials to a guaranty agency. The guaranty agency determines the student's loan eligibility by performing a loan and portfolio review. The guaranty agency mails a loan insurance confirmation to the lender. This action triggers the lender to disperse the funds to the school and to generate a disbursement record form for the guarantor.

If the student defaults on the loan, the lender mails all loan documentation to the guarantor. The guarantor, in turn, mails the defaulted loan documentation to the ultimate loan guarantor, the Department of Education.

Department of Education

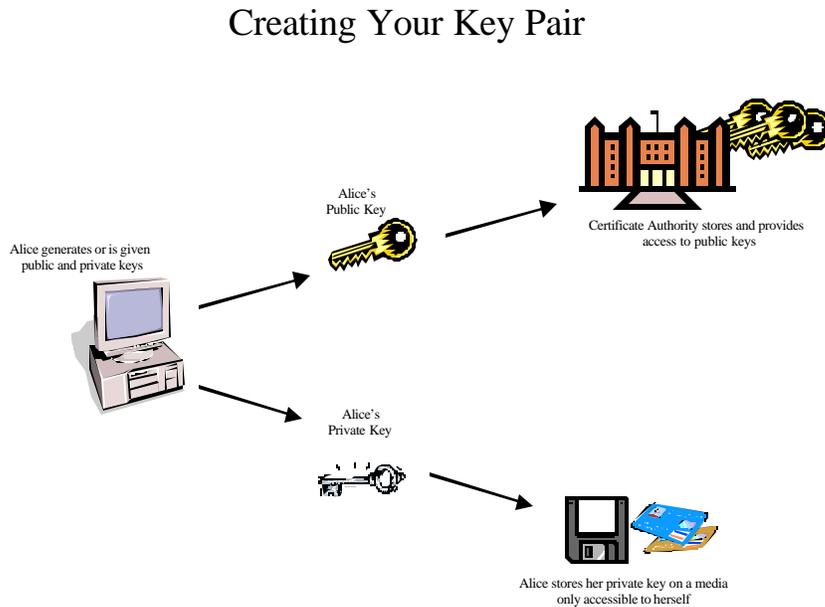
The Department of Education is the ultimate guarantor of every FFEL student loan. During the initial FAFSA submission from the student, ED processes the application, determines the student's loan eligibility, creates a Student Aid Report, and generates a unique student personal identification number (PIN). The Department also generates the Individual Student Information Record (ISIR) for schools to create a total award package for the student. The Department maintains a student's promissory note information for defaulted loans.

Appendix C – An Example of Using the Digital Signature Process

In this example, Alice wants to forward a message to Bob. Alice is concerned with making sure that Bob has a way to ensure that the message was not altered and that Bob can be certain that Alice signed the message contents.¹²

The following is how a digital signature process might work using PKI:

Alice generates or is given a unique public/private key pair.



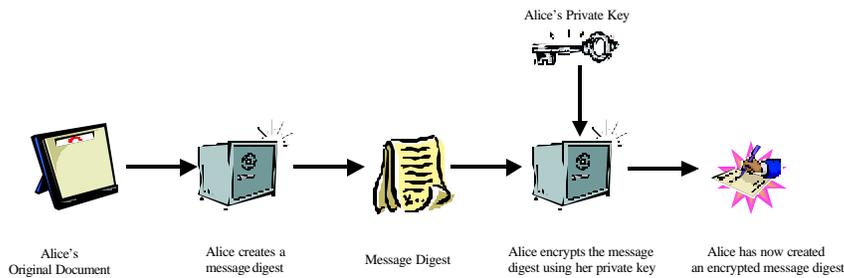
Alice prepares a message (for example, in the form of an electronic mail message) on a computer.

Alice's computer software prepares a "message digest", using a secure hash algorithm. Digital signature creation uses a hash result derived from and unique to both the signed message and Alice's private key. For Alice's hash result to be secure, there must be only a negligible possibility that the same digital signature could be created by the combination of any other message or private key.

Alice applies her private key to the message digest. The private key is applied to the message digest text using a mathematical algorithm. The digital signature is now the encrypted message digest, i.e. digital signature because only Alice's public key can decrypt the encrypted message digest.

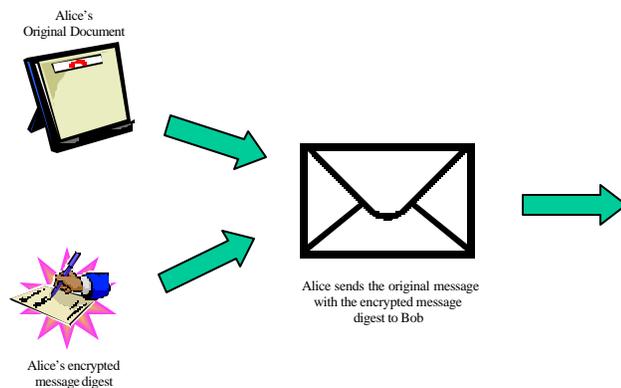
¹² The example Alice, Bob and Eve have become the industry standard for explaining private/public key exchange, encryption and digital signatures, *The Code Book*, Simon Singh, 1999, pg. 257.

Signing a Document



Alice sends Bob the message (encryption or unencrypted), the encrypted message digest and Alice's public key (this is not necessary if Bob already has Alice's public key).

Transmitting a Signed Document

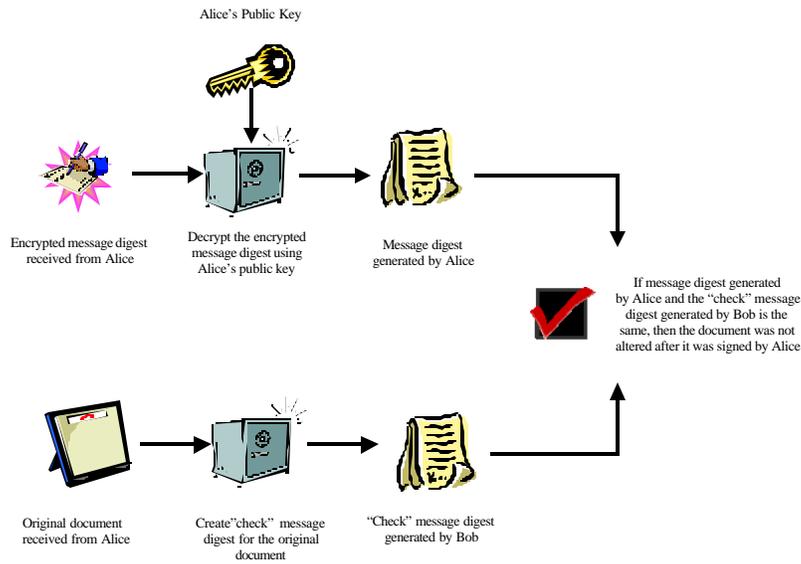


Bob, who has received Alice's digitally signed message and public key, verifies Alice's encrypted message digest by applying Alice's public key to the encrypted message digest to recreate Alice's original message digest. This gives Bob proof that Alice's private key was used to digitally sign the document.

Bob, who now wants to check the integrity of the message, applies the same secure hashing algorithm used by Alice to the original document creating a "check" message digest.

Bob now compares Alice's original message digest against Bob's "check" message digest. If they are the same, Bob knows that the message has not been altered since Alice's private key was used to create the encrypted message digest.

Verification of Digital Signature



Bob wants to make certain that Alice's digital signature and public key have not been revoked (indicating that Alice's private or public has been compromised), Bob can contact the Certification Authority to check the status of Alice's certification.

Appendix D – X.509v3 Digital Certificate Fields

X.509 is based on the use of public-key cryptography and digital signatures. The standard does not dictate the use of a specific algorithm but recommends RSA. X.509 defines a framework for the provision of authentication services by the X.500 directory to its users. The directory may serve as a repository of public-key certificates. Each certificate contains the public key of a user and is signed with the private key of a trusted certification authority. The information contained in the certificate includes a mapping from user name to network address, as well as other attributes and information about the users listed below.

- X.509 Version Number
- Serial Number
- Signature Algorithm ID
- Issuer (Certificate Authority) X.500 Name
- Validity Period (Start and Expiration Dates/Times)
- Subject Name
- Subject Public Key
- Issuer Unique ID – Optional
- Subject Unique ID – Optional
- Extensions – Optional
- Certification Authority's Digital Signature

Appendix E – Digital Signature Proposal Evaluation Issues

Legal

- What are “identity proofing” standards?
- How will you ensure “knowing and meaningful consent”?
- How will evidential trails for electronic documents be supported?
- How will state laws and regulations impact the digital signature process?

Technical

- How is the transaction protected against unauthorized alteration, e.g. records must be accurate and retainable?
- Are the digital certificates software or hardware based?
- What are the hardware and software requirements for the user?
- Are the digital certificates single or multi-purpose?
- How are digital certificates distributed?
- How will electronic transfer of data be supported?
- Is there a contingency plan, in event of system failure?
- Where will electronic transactions be stored?
- What are long-term record retention plans?
- What user documentation will be published to support this initiative?
- Is your organization considering the use of more than one electronic signature option?

Operational

- What information/transaction is being exchanged?
- How does this initiative fit into the SFA Architecture?
- What eMPN documentation will be provided to the student, school and SFA?
- How will you assure that the student, school or SFA have received their required documentation?
- How will schools, students and SFA be notified of changes to the system?
- How will students be notified of the opportunity to use digital certificates?
- How will eMPN transactions be protected?
- How will the proposed system protect the confidentiality of student’s information (privacy)?
- How will the system ensure knowing and meaningful consent?
- Will there be any user fees?
- Who pays the cost of certificate issuance?
- What is the cost of certificate issuance?
- What is the cost of certificate usage?
- Who pays the cost of certificate usage?
- Will a user be able conduct business on paper?
- Are there any additional hardware or software requirements for students, schools or SFA?
- Are there plans to integrate digital certificates into other business processes?
- Why should students accept the use of digital certificates?
- How will success be measured?