Interoperable Digital Identity Management
in the Electronic Exchange of Health Information

An Expert Panel Report

December 17, 2007

With support from:

eHEALTH INITIATIVE
Real Solutions, Better Health

Process and Acknowledgements

This report was written with input from a panel of experts from both health information exchange (HIE) initiatives and digital identity management from the biopharmaceutical, defense and financial services industries, as well as the federal government. The successes in these three industries and the public sector in developing cross-industry trust and identity management processes have helped guide the recommendations for implementing solutions for HIEs in the future. HIE panelists provided invaluable review and practical input that is vital to the implementation of digital identity management solutions within a health information exchange environment. The participation and input of all expert panelists is greatly appreciated.

Members of the expert panel included:

Holt Anderson, North Carolina Healthcare Information and Communications Alliance, Inc.
Nancy Archer, Arkansas Foundation for Medical Care
Mike Berry, HLN Consulting, LLC; Vermont Information Technology Leaders
Malcolm Bertoni, Food and Drug Administration
Carol Bickford, American Nurses Association
Laura Bowser, Gemini Security
Kirk Brafford, Maximus
Kay Bross, Procter & Gamble Company
Rodney Cain, HealthBridge
Vicki Estrin, Vanderbilt Center for Better Health
Jim Hansen, CareEntrust
Peter Hesse, Gemini Security
Al Jackson, RxHub
Joy Jacobsen, CareEntrust
Marc Lassaux, Quality Health Network
Alex Low, United Hospital Fund
Tim Morris, Centers for Disease Control and Prevention
Charles Parker, Masspro
Daniel Pfeifle, Exostar
Eileen Poland, AstraZeneca
Lori Reed-Fourquet, e-HealthSign LLC
Randy Sabett, Sonnenchein Nath & Rosenthal LLP
Gary Secrest, Johnson & Johnson
Mollie Shields-Uehling, SAFE-BioPharma Association
Toby Slusher, Centers for Disease Control and Prevention
Dick Thompson, Quality Health Network
Richard Thoreson, U.S. Department of Health and Human Services
Rich Ware, AstraZeneca
Karen Wendel, IdenTrust
Monroe Wesley, Vanderbilt Center for Better Health
Brian Witt, Arkansas Foundation for Medical Care

Special thanks to Rich Furr, SAFE-BioPharma Association and to Christine Bechtel, Andrew Weniger and Aaron Holman of the eHealth Initiative who supported and conducted research and worked with the many contributors in drafting, editing and completing this paper.

Table of Contents

Executive Summary

The American healthcare system is beginning to recognize the necessity for a reduction in reliance on antiquated paper-based systems and is in the midst of transforming to an interoperable, secure and reliable electronic system. As individual clinicians, hospitals and other care-providing facilities begin to undergo this transformation, new opportunities and challenges arise continually, including in the area of security and identity management.

Secure electronic health information exchange (HIE) across the country is reaching a point which necessitates effective, efficient identity management solutions to address the myriad legal and logistical issues that impact secure, rapid and reliable health data exchange. Other industries have faced this problem in the past and have implemented solutions which may be applicable to an HIE environment. This paper examines factors intrinsically related to identity management in HIE as it relates to clinicians and healthcare providers. While much work remains to be done in the areas of patient identity management and consent to share information, this paper focuses on identity management processes and issues as they relates to care providers in a health information exchange initiative, and draws from what other industries and the federal government have done to address the same issues. The intent of this examination is to provide potential paths forward to address the risks associated with HIE identity management among providers.

Preservation of the security and integrity of health data, while using an interoperable infrastructure, is central to this debate. Wrongful disclosures of electronic health data can be disastrous for both providers and patients. Yet clinicians need access to health data quickly and easily in order to provide care safely and effectively. Therefore, it is necessary for identity management systems to address issues of authentication, authorization, access and audit control. These are the four key cornerstones to any system of trust in a digital environment. How does a system prove someone is who they say they are? If that person is who they say they are, how does a system know what that person should or should not be able to see and do? Beyond these, how does a system track who has seen and done what, and when? The answers to these questions build the basis of trust that is, and will be, needed to support the electronic transfer of health information.

A myriad of factors must be considered when attempting to incorporate digital identity management strategies into the electronic exchange of health information. The federal government provides specific guidance related to the management of identity in an electronic paradigm. The basis of all this guidance is **risk.** System owners must assess the risk inherent in the use, and more importantly the misuse, of the data developed, maintained and archived by any given system. The greater the risk, the more significant the need to assure users' digital identities are tightly bound to individual users in a manner that can assure relying parties (medical professionals, system administrators, payers, auditors, and most importantly, patients) that the data on those systems is protected from exposure.

There are numerous methods to manage identities, control system authentication and authorization for the use of, and access to, specific information and the audit and accounting of who accessed information, when and what did they do with it. These range from simple and rudimentary identity management based on virtually no verifiable information, to much more tightly controlled personal identity verification schema implemented in scenarios in which the risk to data from a number of perspectives is high. After identities have been verified, with the appropriate level of scrutiny, authentication to systems is also possible using an array of methods, again from the simple and relatively insecure to the highly secure and controlled.

Cost and technical complexity were historically the primary barriers for many organizations participating or contemplating participating in exchange. The technology to implement strong identity management has evolved rapidly and the costs have shrunk significantly over the past few years to the point that individual practitioners and almost any HIE can afford implementation. Concomitantly, the technical complexity surrounding public key infrastructure (PKI), arguably the most secure means to manage identities, has also been reduced significantly.

The healthcare industry is unique in a number of ways. Many care providers and facility managers who need access to critical health information are not as easily linked to a single employing entity as say, a scientist in the biopharmaceutical industry. In an environment in which individual clinicians may potentially work for many different care facilities, the need for an identity that transcends regional and employment proximity is necessary. This need also presents a difficult, but not insoluble, problem in developing trust and recognition between facilities. If a nurse or physician, who performs a specific role - for example emergency room staff - works part time at two separate health facilities, are their credentials tied directly to them as an employee of a specific institution, to them as an individual or to them as a subscriber to a larger system of trust? The use of digital identity certificates and federated identity systems provides the means to assure this professional can use their credentials in multiple environments to access the data they require to provide the best quality care at any given time.

A second factor to consider when investigating identity management is the effect on workflow disruption. If a single or two factor authentication process is necessary for a clinician to access health data, that authentication process must readily scale to cover all relevant processes with which the clinician interfaces during the course of a normal day. If not, clinician resistance may be strong, time will be wasted, a care facility's resources needlessly squandered and, most critically, patients may not be afforded the level of care they deserve. The need to confront these issues and provide a single digital identity that quickly and securely interfaces with multiple infrastructures and systems at multiple levels is critical. The ability of systems and infrastructures to support single sign-on will help resolve these issues.

There are a number of systems currently in use in healthcare that provide for authentication and authorization to access health data. How many of these systems interoperate smoothly? HIPAA regulations provide us with a number of structural and legal steps that any care facility must consider when dealing with health data. Many states have also passed and implemented legislation that requires even tighter controls than HIPAA. Illegal disclosures or unauthorized breeches of these sets of data can be costly, and more importantly, they can dramatically set back efforts to mobilize health information to improve patient care. Thus, there is an underlying requirement for system integrity and security that is inherent to the concept of health information exchange. If one facility believes its data systems to be HIPAA compliant and meet other stringent security policies, but is unable to trust that a neighboring facility has afforded the same scrutiny to its systems and policies, that mistrust will reduce the likelihood of effective data exchange. Although this may mitigate legal risk, it does not contribute to the many enhancements technology can bring to healthcare in today's world. While interoperability on a data sharing level is crucial, the ability to build trust in the identity of authenticating users is also critical. Without a common means to assure identity and thereby control authentication and access, the ability to exchange data will be severely limited.

The real benefits accrue as the web of trust expands outward from one organization to encompass the multiple organizations participating in even one HIE. With the malleability of digital media, most authors on the subject state that digitally signed assertions of identity will become the standard.

For most applications that require strong authentication, PKI-based authentication provides the most secure means to meet all requirements. Recent advances in Public Key Infrastructure (PKI) technology provide scalable, reasonably priced options to manage identities in a manner that strongly ties a digital identity, based on a cryptographic certificate, directly to a specific user. Such capability provides relying parties assurance that the person on the other end of the transaction is truly who they purport to be.

Other industries have faced these challenges and opportunities before, particularly in the banking, biopharmaceutical, defense and public sectors. As a result of a review of relevant experience, processes and procedures in these sectors, this paper finds the following:

Recommendations and Findings:

Findings

- HIE has the potential to significantly improve the quality of healthcare, and therefore the health, of the American populace;

- HIE, to be truly successful, requires the application of consistent standards and policies that can work in harmony across state boundaries, including policies for digital identity management;
- Technology continues to evolve, both in identity management and data systems interoperability. As these technologies evolve, health information exchange initiatives will have to maintain awareness of this evolution and can take advantage of these advances.
- Digital identities that are tightly bound to the individual provider offer significant benefits, especially in terms of trust assurance and security, in processes involving authentication to systems outside of a user's parent organization;
- The development of a nationwide network of trust, predicated on strong identity management, is critical to moving HIE forward;
- There are existing models for the development of networks of trust that bear understanding and either implementation or modification to meet HIE needs. It is not necessary to reinvent the wheel.

Recommendations

General Recommendations:

- Awareness of identity management and the need for standard policies and interoperability should be expanded across national public and private sector initiatives, as well as the HIE community;
- Policies and procedures for identity management in HIEs should be further explored and tested in 2008, and lessons learned should be reported to the HIE community.
- To support and foster interoperability, the rules implemented as part of the Federal Common Policy should inform the identity management policies of HIEs.

Members of the SAFE-Biopharma community make the following specific recommendations to HIEs. These recommendations are based on their experience in exchanging sensitive clinical research and other proprietary data between companies, regulators, clinicians and others:

- Form trust networks through a system of closed contracts. The use of a closed contract model provides safeguards by removing enforcement from state or other jurisdictional law, and places it under contract law. It binds members to approved policies and procedures, allows arbitrated dispute resolution, provides the ability to set liability limits and eliminates cumbersome bilateral agreements. This will help address potential issues when HIEs begin to interact with other HIEs as part of a nationwide health information network (NHIN) and provides a common set of policies and guidelines for identity management.
- Develop common policies, procedures and guidelines in order to bind users to them through contracts. The common policies and guidelines developed in closed contract models provide a standard method to manage the life cycle of a digital identity, with specific responsibilities levied on actors in the system at various points. This provides the means to enforce specific actions and consequences for failure to adhere to the rule set. It also provides clear and unequivocal guidelines to all actors for the use of digital identities managed within the system.
- Separate authentication and authorization. Authentication confirms, asserts and validates an identity as being the individual, while authorization grants specific rights based on authenticated identity.
- Authenticate as an individual (vs. organization or role), and authorize based on role. There are a number of ways to implement this recommendation that should be investigated. Roles in digital certificates may present issues in the life cycle management of such credentials that impact the users, especially if their role changes.
- Consider cross-certification with Federal Bridge CA as part of the architecture for NHIN identity management. This would provide interoperability with federal agencies, and potentially provide a platform for use by all networks participating in the NHIN.

1. Introduction

This paper explores the need for, and many of the issues around, identity management and digital signatures for the interoperable exchange of electronic health information. It also explores ongoing transformation in the healthcare industry, in the areas of security of electronic health records – the drivers, the issues, some potential supporting technologies and what other industries are doing in the face of similar challenges. The internet and health information technologies (HIT) offer expanded capabilities, but also present new challenges. Health Information Exchange initiatives will face these same challenges and opportunities.

Health Information Exchange ("HIE") is defined as *the mobilization of health information electronically across organizations within a region or community. HIE provides the capability to electronically move clinical information between disparate healthcare information systems while maintaining the meaning of the information being exchanged. The goal of HIE is to facilitate access to and retrieval of clinical data to provide safer, more timely, efficient, effective, equitable, patient-centered care.*[1]

As the electronic exchange of health information becomes increasingly prevalent, new technology solutions will provide even greater security possibilities, but also require a change in how stakeholders view the entire spectrum of data management. The rapid development of technology, concomitant decreases in costs of implementation. Also, the increasing demand from individuals for more control over data that affects their lives collectively drives a need for the healthcare community to apply lessons learned from other industries as well as the federal government in the area of identity management. There is much to be learned from what others have already developed. Several industries have traveled the same roads upon which the healthcare community is embarking. The roadmaps exist and the trail has been blazed. Effective models exist for establishing trust in healthcare transactions and effectively addressing identity management in a secure, trusted environment.

2. Problem Statement

Secure electronic health information exchange (HIE) across the country is reaching a point which necessitates effective, efficient identity management solutions in order to address the myriad legal and logistical issues that impact secure, rapid and reliable health data exchange. This paper examines factors intrinsically related to identity management in HIE, as it relates to clinicians and healthcare providers. While much work remains to be done in the areas of patient identity management and consent to share information, this paper focuses on identity management processes and issues as they relates to care providers in a health information exchange initiative, and draws from what other industries and the federal government have done to address the same issues. The intent of this examination is to provide potential paths forward to address the risks associated with HIE identity management among providers.

By comparing how other industries and the federal government have addressed these issues, this paper attempts to begin meeting the needs of HIEs by exploring sustainable options in regulating and managing digital identities for providers.

3. Background on U.S. Healthcare System Transformation

The U.S. healthcare system is in the midst of transformation. The long standing reliance on paper records is proving to be not only economically and operationally inefficient, but also detrimental to the health and safety of the increasingly mobile American populace. It is no longer acceptable to rely on

[1] eHealth Initiative *Annual Survey of Health Information Exchange at the State, Regional and Community Levels, 2006.* http://toolkit.ehealthinitiative.org/assets/Documents/eHI2006HIESurveyReportFinal09.25.06.pdf

transferring paper-based health records from provider to provider, especially when a healthcare professional needs critical and timely information at the point of care.

Significant gaps in the safety, quality and efficiency of healthcare have prompted action at the national, state and local levels across the public and private sectors. While recent moves to inject transparency and accountability into provider performance in the dual domains of quality and cost have blossomed, so too have initiatives to mobilize information electronically across multiple settings.

In moving from the exchange of health information on paper to a digital environment, a high level of trust is required to ensure that health professionals requesting and inputting data to electronic patient information are who they say they are. For transactions requiring legal signatures, such as consent forms, prescriptions or physician orders, a signature must:

- be tightly bound to the medical professional's or patient's identity;
- remain accessible in an electronic file;
- be surrounded by a technical process that meets strict legal evidentiary standards.

The integrity of the data in these transactions must also be assured (Is this assured or insured?) so that any post-signature change to any transaction can be readily identified and noted.

In the healthcare field, signatures and data must also comply with relevant HIPAA and other regulatory requirements.

The technology to meet these requirements exists today; it is affordable, it is scalable and available to any HIE. For a given HIE, there may be multiple possibilities – the key to success is identifying and implementing the right solution and policies, especially in a fashion that supports not only the current "local" HIE, but also interconnectivity between HIEs up to and including the Nationwide Health Information Network (NHIN).

4. Key Issues

4.1 The Three A's

Digital identify management is built upon "the Three A's," which are defined as:

4.1.1 Authentication

The confirmation that a user who is requesting services is a valid user of the network services requested. Authentication is accomplished via the presentation of an identity and credentials. Examples of types of credentials are passwords, one-time tokens, digital certificates, and phone numbers.[2]

"Electronic authentication (E-authentication) is the process of establishing confidence in user identities electronically presented to an information system."[3] There are a number of methods that may be used for authentication; however the use of Security Assertion Markup Language (SAML) assertions is growing in application. SAML is an XML standard for exchanging authentication and authorization data between security domains, that is, between an identity provider (a producer of assertions) and a service provider (a consumer of assertions). SAML is a product of the OASIS Security Services Technical Committee.

[2] The Minnesota Privacy and Security Project. Minnesota Department of Health, *A Framework of Principles and Resources for Addressing the Four A's.* April 2007.
[3] NIST SP 800-63, Electronic Authentication Guideline, September 2004

The National Institute of Standards and Technology (NIST) identifies four levels of authentication assurance based on the level of identity authentication, types of identity tokens recommended and the number of factors used in the authentication scheme, each increasingly more secure than the previous.

Just as there are multiple levels of assurance, there are two types of authentication schemes: single-factor and two-factor. Single-factor schemes, characterized by the use of user names and passwords, i.e. something you know, are notoriously simple for hackers and identity thieves to break and compromise. This vulnerability prompted the Federal Financial Institutions Examination Council to issue guidance to the American banking system to strengthen the security of their website authentication schemes by the end of 2006. While this guidance fell short of mandating a move away from single-factor authentication, it strongly suggested they move to two-factor authentication.

In order to understand two-factor authentication, it is important to understand the three methods by which people authenticate themselves to digital systems. There are three universally recognized factors for authenticating individuals:

- 'Something you know', such as a password, PIN, an out of wallet response, shared secret, questions that require a specific user's knowledge to answer or user-selected images identified from a pool of images.
- 'Something you have', such as a mobile phone, credit card, USB, security token or password-generating token.
- 'Something you are', such as a fingerprint, voice, keystroke, a retinal scan or other biometric.

In terms of the electronic exchange of health information, the recently completed first phase of the federally funded Health Information Security and Privacy Collaboration (HISPC) developed expectations based on the A's. The HISPC is a collaborative established under the Agency for Healthcare Research and Quality (AHRQ) meant to address privacy and security policy questions affecting interoperable health information exchanges. The HISPC collaborative includes 35 states, the District of Columbia and two territories. A recent HISPC project report issued by the State of Minnesota included significant emphasis upon the foundation of the A's, in the context of health information exchange[4]. For authentication, one of the key assumptions outlined in the Minnesota report is that: "From the end-user's perspective (i.e. healthcare providers), the authentication of individual access to patients' health information through an HIE should be the same process regardless of which participating organization's health information is being accessed."

More detailed information on authentication is available in Appendix B.

4.1.2 Authorization

Authorization is the granting of specific types of service (including "no service") to a user, based on their authentication, the services they are requesting and the current system state. Authorization may be based on restrictions; for example, time-of-day restrictions, physical location restrictions or restrictions against multiple logins by the same user. Authorization determines the nature of the service which is granted to a user.[5]

In many HIEs, authorization for a given institution is managed first at the HIE organizational level However, authorization for individual institutional providers is often managed within the authorized institution itself. For example, the Minnesota Privacy and Security subgroup notes the following policy: "When an individual is granted access to patients' health information through an HIE from a particular

[4] Minnesota Privacy and Security Project (AAAA Subgroup - 4/30/2007)
A Framework of Principles and Resources for Addressing the four A's. Accessed August 1, 2007, from http://www.health.state.mn.us/e-health/mpsp/index.html#Project%20Reports
[5] http://en.wikipedia.org/wiki/AAA_protocol

organization participating in the HIE, it should be the participating organization's responsibility to authorize, maintain, and terminate the individual's access to patient information."[6]

4.1.3 Accounting

Accounting refers to the tracking of the consumption of network resources by users. This information may be used for management, planning, billing or other purposes. Real-time accounting refers to accounting information that is delivered concurrently with the consumption of the resources. Batch accounting refers to accounting information that is saved until it is delivered at a later time. Typical information that is gathered in accounting is the identity of the user, the nature of the service delivered, when the service began and when it ended.[7]

An additional, fourth 'A' referenced in a white paper by the Minnesota Privacy and Security Project's AAAA subgroup is *auditing.* Auditing is the collection by a system of all instances of access to data - including who accessed it, when it was accessed and any actions taken on the data. This is particularly important as healthcare goes digital and organizations begin connect with one another. To protect both privacy and security, consumers need to know who accessed their information, as well as when and what action was taken with regard to that information. In addition, audit functions continue to be important for organizations in which the collection, access to, manipulation, storage and retention of data is controlled by regulatory agencies, such as the Food and Drug Administration (FDA), the Centers for Medicare & Medicaid Services, etc. The evidence of these activities is maintained in an audit trail that is created by the system and must be available to regulatory and internal auditors in human readable format for the life of the data. For example, Minnesota's HIE-specific guidance outlines three principles that HIEs should develop and accept:

> a) the data elements to be maintained and exchanged for auditing individuals' access to patient health information;
> b) the frequency at which the auditing data will be exchanged between organizations participating in the HIE; and
> c) the minimum retention time of audit logs maintained for auditing individuals' access to patient health information."[8]

4.2 The need for trust: What is trust?

Figure 1 graphically portrays a crucial problem with identity management on the Internet. *How does a system, or a relying party, know for sure the person on the other end of a transaction is who they say they are?* The baseline for assuring security is a system of trust that ensures, to the maximum degree possible, the individuals who are provided such access are, in fact, the individual they purport to be. In other words, the identity of the individual who can access patient data, for whatever purpose, must be verified initially with a high degree of assurance and then, tightly bound to whatever "credential" they use to access records. Tight controls must be in place to ensure that only authorized users with verified identities may authenticate to systems that collect, store, process, maintain and archive health-related information. There are a number of schemas to perform what is known as identity authentication.

---

[6] Minnesota Privacy and Security Project (AAAA Subgroup - 4/30/2007)
A Framework of Principles and Resources for Addressing the four A's. Accessed August 1, 2007, from http://www.health.state.mn.us/e-health/mpsp/index.html#Project%20Reports
[7] HIMSS/GSA. *National e-Authentication Project Whitepaper.* June 2007.
[8] Minnesota Privacy and Security Project (AAAA Subgroup - 4/30/2007)
A Framework of Principles and Resources for Addressing the four A's. Accessed August 1, 2007

The verification of an individual's identity is paramount to the development and operation of any system of trust. The federal government and several industry initiatives have all begun with this as the cornerstone of their systems. This paper discusses such approaches to identity authentication in subsequent sections.

Figure 1. Identity on the Internet

4.2.1 Healthcare and Trust: Sensitivity and Necessity

Data Sensitivity is defined as the stated and implied expectation around integrity and disclosure of health information. This sensitivity is usually addressed at the institutional level and where HIE is underway or contemplated; it is also important at an inter-organizational level. Data sensitivity is addressed by designing and implementing appropriate security measures throughout the lifecycle of the information.

Healthcare institutions generally refer to a combination of HIPAA and Information Security best practices to govern the approach they take to integrity and disclosure within the institution.

When HIE is either underway or contemplated, the same foundation of HIPAA and Information Security best practices apply, however, there are many different implementations undertaken to achieve verifiable integrity and appropriate disclosure of health information. Most HIE services or functions (such as lab results delivery, medication history, clinical messaging, etc.) involve disclosure of personally identifiable information for purposes of clinical care. As such, the HIPAA rules allow disclosure to individuals and institutions governed by appropriate Business Associate and Data Use Agreements. There are often misunderstandings, with some HIEs becoming distracted by the HIPAA prohibitions against inappropriate disclosure of personal health information (PHI).

Given these data sensitivity requirements for HIEs, there is a compelling case for a reasonable level of identity proofing for the participants in an HIE.

4.2.2 Data Integrity

Data integrity and the ability to know when data has been changed in any way and by whom is crucial. Systems must maintain audit logs to track any activity related to data maintained by those systems. However, the individual user has no real knowledge of the integrity of data since they rarely, if ever, have access to these audit logs. There simply is no easy way for the user to know if data have been changed without some type of technology that can immediately detect change and advise the user that change has occurred. This is especially important when dealing with data, documents or records that have been signed and certified as accurate, such as a person's medical records signed by a doctor or other medical professional.

4.2.3 Non-repudiation

In its legal review of digital signatures in 1996, the American Bar Association (ABA) defines non-repudiation as "strong and substantial evidence of the identity of the signer of a message and of message integrity, sufficient to prevent a party from successfully denying the origin, submission or delivery of the message and the integrity of its contents."[9] The ABA further defines a "message" as any digital representation of information, e.g., electronic health records, electronic prescriptions, electronic physician orders, etc. User name and password and other weaker forms of credentials simply do not provide the legal strength to support strong non-repudiation.

In the HIE environment, non-repudiation is especially important because of the nature of the records involved. In cases of disputes, civil or criminal proceedings or adjudication of claims for treatment, it is important that signatures on records or data be tightly bound to the signatory and that the signatory is not able to readily disavow that signature.

4.2.4 Security

On August 12, 1998, HHS published a proposed rule (63 FR 43242) to establish a minimum standard for security of electronic health information. The proposed rule established a standard that would require the safeguarding of all electronic health information by covered entities. The proposed rule included a standard for electronic signatures used as a means to secure information and data. The final rule published on April 21, 2003 adopted only security standards. According to HHS, all comments concerning the proposed electronic signature standard, responses to these comments and a final rule for electronic signatures will be published at a later date.

The proposed rule stated the following:

"If an entity elects to use an electronic signature in a transaction as defined in § 142.103, or if an electronic signature is required by a transaction standard adopted by the Secretary, the entity must apply the electronic signature standard described in paragraph (b) of this section to that transaction.

(b) Standard.

(1) An electronic signature is the attribute affixed to an electronic document to bind it to a particular entity. An electronic signature secures the user authentication (proof of claimed identity) at the time the signature is generated; creates the logical manifestation of signature (including the possibility for multiple parties to sign a document and have the order of application recognized and proven); supplies additional information such as time stamp and signature purpose specific to that user; and ensures the integrity of the signed document to enable transportability of data, interoperability, independent verifiability, and continuity of signature capability. Verifying a signature on a document verifies the integrity of the document and associated attributes and verifies the identity of the signer.

[9] American Bar Association, Legal Infrastructure for Certification Authorities and Secure Electronic Commerce, 1 August 1996, Section 1.20

(2) The standard for electronic signature is a digital signature. A "digital signature" is an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters so that the identity of the signer and the integrity of the data can be verified."

As of this date, the final rule for digital signatures has not been published. In the absence of this rule, the use of digital signatures is loosely guided by the Electronic Signatures in Global and National Commerce Act (ESIGN) and the Uniform Electronic Transactions Act (UETA). It is important to note that ESIGN applies to contracts involved in interstate and international commerce. UETA was developed by the National Conference of Commissioners on Uniform State Laws and has been passed by most of the states. While both apply mostly to contracts, the implications for electronic signatures may be implied for other forms of electronic records.

To achieve the basic purposes of signatures outlined above, a signature must have the following attributes:

- **Signer authentication**: A signature should indicate who signed a document, message or record and should be difficult for another person to produce without authorization.
- **Document authentication:** A signature should identify what is signed, making it impracticable to falsify or alter either the signed matter or the signature without detection.[10]

The use of digital signatures usually involves two processes, one performed by the signer and the other by the receiver of the digital signature:

- **Digital signature creation** uses a hash result derived from and unique to both the signed message and a given private key. For the 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.
- **Digital signature verification** is the process of checking the digital signature by reference to the original message and a given public key, thereby determining whether the digital signature was created for that same message using the private key that corresponds to the referenced public key.[11]

The processes of creating a digital signature and verifying it accomplish the essential effects desired of a signature for many legal purposes:

- **Signer authentication**: If a public and private key pair is associated with an identified signer, the digital signature attributes the message to the signer. The digital signature cannot be forged, unless the signer loses control of the private key (a **compromise** of the private key), such as by divulging it or losing the media or device in which it is contained.
- **Message authentication**: The digital signature also identifies the signed message, typically with far greater certainty and precision than paper signatures. Verification reveals any tampering, since the comparison of the hash results (one made at signing and the other made at verifying) shows whether the message is the same as when signed.
- **Affirmative act**: Creating a digital signature requires the signer to use the signer's private key. This act can perform the ceremonial function of alerting the signer to the fact that the signer is consummating a transaction with legal consequences.
- **Efficiency**: The processes of creating and verifying a digital signature provide a high level of assurance that the digital signature is genuinely the signer's. As with the case of modern electronic data interchange (EDI) the creation and verification processes are capable of complete automation (sometimes referred to as machinable), with human interaction required on an exception basis only. Compared to paper methods such as

[10] American Bar Association, Digital Signature Guidelines, Legal Infrastructure for Certification Authorities and Secure Electronic Commerce, August 1, 1996
[11] Ibid.

checking specimen signature cards -- methods so tedious and labor-intensive that they are rarely actually used in practice -- digital signatures yield a high degree of assurance without adding greatly to the resources required for processing.

The reason the proposed rule stipulated digital signatures is that only a digital signature supports the processes required to ensure document integrity and non-repudiation.

It is also worthy of note that the Centers for Medicare & Medicaid Services has prepared guidance to provide HIPAA covered entities with general information on the risks and possible mitigation strategies for remote use of and access to Electronic Protected Health Information (EPHI).[12]

5. Health Information Exchange and the Need for Trust

5.1 What is HIE?

A number of states, regions and communities across the United States are mobilizing healthcare information across organizations to improve health and healthcare through multi-stakeholder collaborative efforts. These initiatives involve a broad range of participants, including hospitals and other healthcare providers, physician practices, health plans, employers and other healthcare purchasers, laboratories, pharmacies, public health agencies, state and local governmental agencies and most importantly, patients.

Health information exchange (HIE) is defined as the mobilization of healthcare information electronically across organizations within a community. HIE provides the capability to electronically move clinical information between disparate healthcare information systems while maintaining the meaning of the information being exchanged. The goal of HIE is to facilitate access to, and retrieval of, clinical data to provide safer, more timely, efficient, effective, equitable, patient-centered care.[13]

Formal organizations are now emerging to provide both form and function for health information exchange efforts. These organizations (also called Regional Health Information Organizations, or RHIOs) are ordinarily geographically-defined entities which develop and manage a set of contractual conventions and terms, arrange for the means of electronic exchange of information, and develop and maintain HIE across community boundaries.

HIEs or RHIOs have emerged as vehicles to facilitate the flow of clinical information between providers in the community; they are building on the foundation laid by the pioneers in the field - the Indiana Health Information Exchange, the Inland Northwest Health System, HealthBridge and others. The primary business focus of these exchanges creates value for the provider community by fostering administrative efficiencies. In doing so, the aforementioned HIEs are unusual because they have been able to generate modest revenue, and therefore have achieved a modest but sustainable business model.

HIEs are currently responding to a simple but important need in the market, helping providers with disparate clinical information systems and siloed clinical databases to find information on a patient that resides in that community. With the development of a Nationwide Health Information Network (NHIN) integrating HIEs and RHIOs, it may become possible to provide the same capability across communities.

This need has been spurred by countless observations and studies suggesting that patient care is simply not coordinated between the providers caring for the patient; that tests and studies on individual patients are unnecessarily duplicated; and that patients are constantly at risk of being harmed by the healthcare system because critical information on their health status is not easily accessible and considered when decisions about their care are undertaken.

[12] http://www.cms.hhs.gov/SecurityStandard/
[13] eHealth Initiative, Annual Survey of Health Information Exchange. Washington DC, 2005.

5.2 What are the recent trends?

Within the context of the development of HIEs across the country, there has been an increased emphasis on security and privacy of the information accessed within the HIEs and development of sustainable business models for these entities. Several high profile HIEs have been terminated due to less than adequate community participation in the HIE.

Security and Privacy: While individual HIEs have not been terminated due to security and privacy concerns, the general public and HIE stakeholders in particular have applied an increasingly demanding standard of care to the subject. Two works associated with this effort include the Markel Foundation's "Connecting for Health Common Framework"[14] and the HISPC project. Both projects reached similar conclusions concerning the high standard of security and privacy needed to ensure community support for, and reliance upon, HIE as a viable mechanism for accessing healthcare information about patients.

From the "Connecting for Health Common Framework" we find this summary of the expectation:

> *A 21st century health information environment should earn and keep the trust of the public through policies that provide safeguards and transparency. Americans will support sharing their sensitive health information across the Internet if they trust in the security, privacy, and appropriate use of the network. Such trust can be established through a combination of safeguards (including both technical and non-technical approaches) and transparency (of both decision making process and practice). The technical architecture will include tools protect data against break-ins and theft to provide anonymization, and to prevent data corruption or error. The policy architecture will develop clear rules and guidelines through an inclusive and transparent ongoing process.*

Sustainable Business Models: Simultaneous with the increased emphasis on Security and Privacy, HIEs have found that a robust business model is critical to their ongoing survival. The most elegant technical solution will have limited usefulness if it fails to deliver net value to the community served. The recent trends have included an ever increasing acknowledgement of the importance of business planning to the success of HIEs. The post-mortem of the Santa Barbara experiment recently published in *Health Affairs*[15] presents a clear example of this emphasis on the need for a compelling economic support for a community based HIE.

In order to build a sustainable business model for HIE, in addition to the foundation of reliable security and privacy, the HIE must provide a suite of services valued by the community for their incremental improvement to the safety, quality and efficiency of health and care for the patients in the served area. Continued support for the HIE is dependent upon continued proof of this value equation, be it based on delivery of administrative efficiencies or more complex values.

Trends: Shared priority between ensuring security and privacy while conducting the operations of the HIE as a "business" with the concomitant acknowledgement of market forces which may impact all other priorities of the HIE is becoming the norm.

Because HIEs continue to be nurtured across the country as a means to address pain points in healthcare delivery, it is logical to expect that these HIEs will increasingly focus on the foundational elements of adequate security and privacy and development of a sustainable business model.

A continuation of the HISPC project is currently underway, and HIEs can expect the conclusions reached during this project to continue to raise the bar for security and privacy as well as further clarify the expectations of all involved stakeholders.

The increasing mobility of the American populace mitigates for a national network that will support patient care data accessibility and transparency. The Nationwide Health Information Network must evolve to provide support for the need of providers in all areas of the country to have immediate access to an individual record regardless of its original source. Digital identities, managed within a structured system

[14] http://www.connectingforhealth.org/commonframework/
[15] http://content.healthaffairs.org/cgi/content/abstract/26/5/w568

to ensure their control, provide a means to this end. Using a system of trust based on an individual's digital identity allows implementation of the Four A's in a way to ensure security and privacy are maintained at all levels. Additional sustainability support is expected to arise from the interoperability of HIEs which may provide an additional resource for revenue generation through the HIEs serving as an aggregator of health information.

5.3 Case Studies

Case Study: Indiana Health Information Exchange (IHIE)

IHIE relies on the security procedures at participating hospitals to manage the authentication, authorization, accounting/access control and auditing of clinicians accessing health information through the IHIE system. In the IHIE, unaffiliated clinicians are managed centrally by the HIE itself.

Thus, authentication is performed one of two ways:

A) Distributed – operational responsibility lies with participating institution (such as hospitals) using their internal security policies and procedures, which meet IHIE's standards and have contractually committed to the 4A's (60-80 % of all users).

B) Centralized – IHIE-administered, which includes two physical visits to the clinician's office, review of fiscal and professional background for the individual, face to face verification and hand delivery of a username and password to the individual.

IHIE has experimented with biometric and other two-factor authentication, but determined that clinician resistance and costs outweighed usefulness at this time. IHIE has also investigated using third party notaries for verification of individuals – with a 70% failure rate. Future plans include significant improvements, including perhaps two factor authentication.

Case Study: MidSouth eHealth Alliance (MSeHA)

Authentication is performed in a distributed operation: Authentication and identity management of users within MSeHA is currently performed by a committee of participants, most of which are part of MSeHA's *Operations Committee.* All users that require authentication must be associated with at least one participant of MSeHA, such as a participating hospital, which will attest for the user's verification.

Usernames and RSA secure, two factor authentication tokens are issued to all affiliated and confirmed individuals by MSeHA central management. All identity management processes following the authentication of a user, such as access right changes, regular reviews, unusual behavior awareness, etc. are the responsibility of MSeHA.

Although it plans to continue the use of a username and RSA SecurID, or other two factor authentication system for all users outside of a participant's network, MSeHA is considering in the future relying on a mixed model of trusted authentication that would possibly pass a network username from a participant via a secure access path, or digital certificate, to the MSeHA and require a four digit PIN for access.

Case Study: Connecticut Health Information Security and Privacy Initiative (CT-HISPI)

Authentication: The CT-HISPI is in the process of developing specifications, policy and process re-engineering to establish a healthcare Workforce Identity Management and Authentication Service tied to entity and practitioner licensure and corporate workforce identity solutions. This project aims to provide trusted digital identities for authentication, authorization, access control, data integrity and digital signature purposes.

In order to enable interstate HIEs, it is important to be able to identify the requester of information with an elevated assurance. Therefore it is appropriate to attach the provider identification to their healthcare licensure, especially since all healthcare providers are regulated and managed at the state level. This effort will enable the use of ISO IS17090 Health Informatics PKI to issue the digital identities to the state's healthcare workforce. This international standard is cited by IHE interoperability profiles related to provider identification and will be interoperable with those solutions provided by the health information technology vendors. These identities would be issued on FIPS 140-2 compliant tamper resistant media allowing for a high assurance level of the requestor identity and medical credentials can be associated with the requestor of the information. This will offer the information resource two-factor authentication capabilities.

The policy will also require that the certification authority selected for issuing the ISO IS17090 compliant identities be cross-certified with the Federal Bridge. This will enable interoperability with government agencies and federal systems as well as across state lines. Policies and workflow processes will also be closely aligned with the licensure life cycle because the Connecticut Department of Public Health is the authority responsible for regulated practitioner credentials.

Specific project objectives for this solution include:
1. Development of systems specifications for integration with the professional healthcare licensure process and integration with provider workforce identity management systems;
2. Adoption and incorporation of national standards to represent the core concepts that influence provider/workforce authorization decisions; and
3. Coordination with multi-state digital identity efforts. Final specifications will be written in a manner such that other states will be able to incorporate Connecticut's specifications as a “How to Guide” to streamline the development process in other states and encourage adoption of common policies, standards and processes that further interstate HIE.

When fully implemented, the final solution hopes to:
1. Enable trusted remote identification and authentication across digital locals;
2. Support physical access security mechanisms (including homeland security/bioterrorism scenarios);
3. Enable trusted digital signatures, including all tiers of prescriptions; and
4. Incorporate workforce credentials and employer role authorizations or 'agency' (a business or service authorized to act for others).

Case Study: CareEntrust

Initial activation of accounts requires a 32 digit random key that is delivered via U.S. mail or e-mail, as well as the input and verification of personal information to create a unique login name and password. CareEntrust does not currently require a second factor authentication. This is because the current version of Oracle Identity Management (IM), the primary identity management software utilized by the HIE, does not provide for two-factor authentication. CareEntrust’s technology supplier is currently migrating from an Oracle to an IBM-based portal solution. Once the transition is made, an assessment of IBM supplied and certified third party solutions will be evaluated to support second factor authentication. In the interim CareEntrust is also looking at performing a “1.5 factor authentication” level where previously answered security questions are randomly posed to the user at login.

5.4 Analysis: Identity Management and HIEs

In order to understand some of the security efforts underway in HIEs today, we have examined the procedures of several operating HIEs. While variety in implementation is expected, consistency in approach was noted across the implementations at Indiana Health Information Exchange (Indiana), MidSouth eHealth Alliance (Memphis), and CareEntrust (Kansas City). This consistent approach as documented in detail in Appendix A can be summarized as follows:

Administration of identity management: Every HIE must employ specified procedures to manage access to the information in the HIE. In most existing models, the primary means are focused on distributed or centralized procedures.

With the exception of clinicians unaffiliated with any of the participating institutions, verification of authentication to systems, authorization to access specific data on those systems, and development and maintenance of audit records is managed on a distributed basis by the participating institution(s) with which the clinician is affiliated. The central HIE relies on the authentication, authorization, accounting/access control and auditing procedures in place at the participating institutions.

5.4.1 Credentialing issues

HIEs generally use various authentication methods to attempt to ensure access to the information delivered by the HIE is limited to specific individuals. The HIE must be able to guarantee the identity of the person using the system. To achieve this level of assurance, several HIEs have experimented with sophisticated credentialing processes and the implementation of mechanisms such as two factor authentication. However, it is worthy of noting that most HIEs do not use strong authentication methods.

A variety of factors, including the evolution of identity management standards and the ongoing HISPC efforts, provide the impetus and capability to provide significantly stronger assured identities in the electronic environment. The ongoing HISPC reports will continue to raise the bar for authentication within HIEs. For example, many of the HISPC projects are currently studying the impact of HIE specific consent forms used by patients participating in HIEs. The implications of using these consent forms will include increased transparency into the security and privacy efforts of the HIEs; yet another way the bar will be raised. The communities, and especially consumers, will become even more aware of the security and privacy risks and may advocate for even stronger identity management solutions as a result of being "reminded" of the risks by the consent forms.

Other industries and the federal government have also realized the need to support processes for identity verification that, while maintaining strong assurance, do not impose onerous requirements on individuals. In recognition of this, they allow the use of antecedent data, i.e., data based on previous face to face identity vetting that is maintained by trusted sources that can be parsed to ensure requirements are met. An example for medical professionals would be state licensing authorities that require the presentation of picture id in a face to face setting to verify the identity of the applicant. The data derived from this process can be accessed via electronic means and serve to meet the requirements for basic, and medium assurance identity management. This is the process SAFE is implementing as it moves to a tiered services model.

5.4.2 Costs of implementing trust assurance systems

HIEs have a hard time developing and implementing business models that support their ongoing financial viability. The vast majority of HIEs in development and underway throughout the country are funded for a limited period of time, if at all. Therefore, many HIEs have considered implementing robust digital identity management as a nice to have, and have relied on some form of single factor authentication.

The pressures to demonstrate a financially sustainable business model and respond to an ever increasing demand for robust security and privacy places many HIEs in a position to balance risks versus costs. Fortunately the costs associated with digital identity management have been dropping concurrently with increasing demand for assured identity. There are now third party sources that will provide identity management and credential management services for a contracted fee at a level that is within the means of most HIEs. There are also third parties that will provide complete end-to-end PKI services at a cost that is significantly lower than the dated costs most often cited to stand up an internal PKI. The ease or difficulty of balancing the economics of security and privacy remains unknown, but is a focus for efforts like the project generating this paper.

5.4.3 Workflow challenges with implementation

HIEs face a complex situation of reliance upon their participating institutions to appropriately conduct the Authentication, Authorization, Accounting and Auditing. This reliance is mirrored in the other industries such as banking, where the participating institutions rely on an interlocking set of systems and processes to ensure the integrity of the entire network.

Ensuring collaboration and consistency in the decentralized model is both a policy and practical matter. The "trust and verify" approach provides assurance to the central HIE that the participating organizations do, in fact, implement and use policies and practices to ensure security and privacy. Each participating entity should be subject to audit from the HIE to ensure that those policies and procedures are being followed adequately. Additionally, HIEs should consider establishing prevent controls designed to alert the HIE if lapses in security procedures occur at participating institutions. An example of a prevent control is the submission of a copy of the checklist for authentication documenting that the participating institution followed all relevant procedures to authenticate a new user.

Above and beyond implementation workflow challenges are those related to providing *value added incentives* for the use of a digital ID management system. Many HIEs, as well as EHR vendors and developers, have found it difficult to increase physician participation in such things as public health disease registries because of workflow complications. Many HIEs have remarked that it is difficult to get a provider to switch between an EHR system to a web-based registry and back if their infrastructures do not support single sign on and there is no financial incentive for using these systems. To incent practitioners, some public health agencies have developed financial rewards for adding data to a registry. By using a digital identity management system based on a universal digital identity, and mitigating workflow disruptions, value added incentives to increase participation in certain programs like disease registries can be implemented. Simplification of these processes may reduce the perception that they delay care, and they may potentially be seen as a bonus step in regular workflow.

5.4.4 Interoperability given current environment

Given the nascent status of HIEs, the realization of interoperability remains an elusive goal. The Nationwide Health Information Network (NIHN) project is providing technical means, but more importantly process and procedural means, to provide for interoperability between isolated points on a nationwide network. Additionally, the recent HISPC final report[16] notes that "…the lack of interoperability across systems for purposes of identifying providers, which forces a patient's providers to "jump" from one system to the next to gather and manually integrate all the information available on him or her instead of using automated methods to aggregate the information across sources." This lack of interoperability facilitates administrative overhead as providers are forced to log on and off different systems to aggregate information (if the information is electronic to begin with).

Interoperability between HIEs, while needed, is not the highest priority for most HIEs, as most are focused on establishing themselves within a defined medical trading area/community. This lack of focus may provide an unwelcome opportunity for inconsistent implementations, which may result in limits on the continuing objective of interoperability while incorporating standards as they are developed and deployed. Such an approach, if it results in multiple infrastructures that cannot easily interoperate at all levels, will prevent the development of a true Nationwide Health Information Network.

Most of the "early adopters" of health information technology who are willing and able to experiment with new procedures and technologies that increase the quality of care, have begun to realize unforeseen benefits. In terms of stimulating adoption rates, aside from upfront funding sources by state and federal governments, increased access to data between and across HIEs can decrease repetitive costs and increase efficiency in delivered care. However the lack of federated and interoperable digital authentication systems limits this flow of data. To cite only one example, the ability of an emergency

[16] http://healthit.ahrq.gov/images/jul07nationwidesummary/nationwide.htm

room staff to see a patient's previous discharge data from a different facility will ultimately lead to improved care and greater savings.

5.4.5 Standards –state of existing standards, need for adoption

There are few standards for digital identity management within an HIE environment. Standards require both a policy and a technical framework to be effective. At the present time, the technical part of standards work is moving forward under the auspice of organizations, such as the Health Information Technology Standards Panel (HITSP) and HL7. The policy aspects, however, are not as well defined and require much more effort and detail. Organizations such as the Office of the National Coordinator (ONC), the American Health Information Community (AHIC) and the Health Information Security and Privacy Collaboration (HISPC) are all working to develop the required policies. The Certification Commission for Health Information Technology (CCHIT) is responsible for developing and evaluating certification criteria for HIT in three different areas[17]:

- Ambulatory EHRs for the office-based physician or provider
- Inpatient EHRs for hospitals and health systems
- The network components through which they interoperate and share information

The standards built into the electronic health records which have been certified by the CCHIT stand as one of the few means by which secure digital transfer can be measured. Recommendations by the CCHIT to the American Health Information Community (AHIC) in March of 2007 outlined a number of requirements for digital access, audit and authentication to ambulatory and inpatient EHRs that stand as the greatest indicators of where digital identity management is headed in the HIE realm.

Not all the approved requirements by the CCHIT are relevant to the issue of digital identity management within an HIE, however selective requirements can be seen as indicative of what future requirements may develop. These standards are doubly important as they both indicate the road ahead for HIEs, and also govern the expectations which can be placed upon systems used for decentralized user identity verification and management as described in Appendix A.

In terms of **authentication**, the following requirements apply to digital identity management:

- Authenticate the user before any access to Protected Resources (e.g. PHI) is allowed, including when not connected to a network e.g. mobile devices.
- When usernames and passwords are used to authenticate a user:
    - Support password strength rules that allow for minimum number of characters, and inclusion of alpha-numeric complexity.
    - Provide an administrative function that resets passwords when passwords are used. When passwords are used, user accounts that have been reset by an administrator shall require the user to change the password at next successful logon.
    - Provide only limited feedback information to the user during the authentication.
    - Support case-insensitive usernames that contain typeable alpha-numeric characters in support of ISO- 646/ECMA-6 (aka US ASCII).
    - Allow an authenticated user to change their password consistent with password strength rules (S13).
    - Support case sensitive passwords that contain typeable alpha-numeric characters in support of ISO-646/ECMA-6 (aka US ASCII).
    - Not store passwords in plain text.
    - Prevent the reuse of passwords previously used within a specific (configurable) timeframe (i.e., within the last X days, etc. - e.g. "last 180 days"), or shall prevent

[17] Certification Commission for Health Information Technology (CCHIT) website: http://www.cchit.org

the reuse of a certain (configurable) number of the most recently used passwords (e.g. "last 5 passwords").

- Upon detection of inactivity of an interactive session, prevent further viewing and access to the system by that session by terminating the session or by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures. The inactivity timeout shall be configurable.
- Enforce a limit of (configurable) consecutive invalid access attempts by a user. The system shall protect against further, possibly malicious, user authentication attempts using an appropriate mechanism (e.g. locks the account/node until released by an administrator, locks the account/node for a configurable time period, or delays the next login prompt according to a configurable delay algorithm).
- Support two-factor authentication in alignment with NIST 800-63 Level 3 Authentication. Note: The standards in this area are still evolving.[18]

In term of **authorization**, EHR requirements that may be relevant to digital identity management include:[19]

Systems must;

- Enforce the most restrictive set of rights/privileges or accesses needed by users/groups or processes acting on behalf of users, for the performance of specified tasks.
- Provide the ability for authorized administrators to assign restrictions or privileges to users/groups.
- Associate permissions with a user using one or more of the following access controls: 1) user-based (access rights assigned to each user); 2) role based (users are grouped and access rights assigned to these groups); or 3) context-based (role-based with additional access rights assigned or restricted based on the context of the transaction such as time-of-day, work station location, emergency-mode, etc.)
- Support removal of a user's privileges without deleting the user from the system. The purpose of the criteria is to provide the ability to remove a user's privileges, but maintain a history of the user in the system.

In terms of **auditing** abilities, the following requirements are relevant to digital identity management:

- Detect security-relevant events that it mediates and generate audit records for them. At a minimum the events shall include: start/stop, user login/logout, session timeout, account lockout, patient record created/viewed/updated/deleted, scheduling, query, order, node-authentication failure, signature created/validated, PHI export (e.g. print), PHI import, and security administration events. Note: The system is only responsible for auditing security events that it mediates. A mediated event is an event that the system has some active role in allowing or causing to happen or has opportunity to detect. The system is not expected to create audit logs entries for security events that it does not mediate.
- Record within each audit record the following information when it is available: (1) date and time of the event; (2) the component of the system (e.g. software component, hardware component) where the event occurred; (3) type of event (including: data description and patient identifier when relevant); (4) subject identity (e.g. user identity); and (5) the outcome (success or failure) of the event.
- Provide authorized administrators with the capability to read all audit information from the audit records in one of the following two ways: 1) The system shall provide the audit records in a manner suitable for the user to interpret the information. The system shall provide the capability to generate reports based on ranges of system date and time that audit records were collected. 2) The system shall be able to export logs into text format in such a manner as to allow correlation based on time (e.g. UTC synchronization).

[18] CCHIT 2007 Final Criteria, March 16, 2007. Certification of EHRs
[19] CCHIT 2007 Final Criteria, March 16, 2007. Certification of EHRs

- Support time synchronization using NTP/SNTP, and use this synchronized time in all security records of time.
- Have the ability to format for export recorded time stamps using UTC based on ISO 8601. Example: "1994-11-05T08:15:30-05:00" corresponds to November 5, 1994, 8:15:30 am, US Eastern Standard Time. (provisional requirement)
- Prohibit all users read access to the audit records, except those users that have been granted explicit read-access. The system shall protect the stored audit records from unauthorized deletion. The system shall prevent modifications to the audit records.
- Allow an authorized administrator to enable or disable auditing for groups of related events to properly collect evidence of compliance with implementation-specific policies. Note: In response to a HIPAA-mandated risk analysis and management, there will be a variety of implementation-specific organizational policies and operational limits. (provisional requirement)
- Support logging to a common audit engine using the schema and transports specified in the Audit Log specification of IHE Audit Trails and Node Authentication (ATNA) Profile
- Support access to blinded information to a treating clinician, when the blinded information is necessary for managing an emergency condition. Note: This is commonly known as a "break the glass" function. This does not provide increased access rights for the user. The "break the glass" function must be capable of requiring the clinician requesting access to blinded information to document and record the reason(s) for requesting access.[20]

6. The Current State of Trust

6.1 How can Trust be Managed? Alternatives

Most of the issues previously discussed can be managed today using a number of technologies ranging from simple user name and password up to and including PKI-supported biometrics.

The entire matter of trust is complicated significantly when moving from closed systems, such as those operated by a care facility in which access is limited to a known group of users (e.g., medical professionals who are employees or have staff privileges), to open systems such as those operated by a single HIE, or more significantly a National Health Information Network. In the latter two instances, access is no longer limited to a small “known” group of users, but rather access may be required by users completely unknown to the operator of the infrastructure. How can such a complicated task be managed effectively?

User names and passwords work well for instances of closed systems. The system administrators can manage access based on user name and password, the assignment of user names and passwords can be controlled and linked fairly readily to the individuals who access these networks since they are generally all known individuals to the operating organization and have, most likely gone through some level of identity vetting prior to being assigned user names and passwords. The primary problem with user names and passwords in open systems is that they are notoriously insecure. They are subject to attack by even relatively unsophisticated hacking as is practiced today by installing eavesdroppers such as key stroke loggers and other forms of malware.

As noted by Matt Blaze, et al of the AT&T Research Labs in their paper, The Role of Trust Management in Distributed Systems Security, “in an operating system the identity of a principal is well known. This is not so in a distributed system where some form of authentication has to be performed before the decision to grant access can be made. Typically authentication is accomplished via a user name and password mechanism. Simple password-based protocols are inadequate in networked computing environments, however, even against unsophisticated adversaries, simple eavesdropping can destroy security.

[20] CCHIT 2007 Final Criteria, March 16, 2007. Certification of EHRs

Other recently developed mechanisms include:

- One time passwords, which do not secure the rest of a user session beyond authentication;
- Centralized ticket systems such as Kerberos (MNSS87). Problems with such systems include the necessity for an authentication server (and for frequent communications with it) and implicit trust assumptions;
- Public key based protocols which are considered the "state of the art" for scalable authentication systems." [21]

Closed systems were generally implemented on a single server system using operating system-level security. They are neither flexible nor scalable enough to handle today's requirements for internet-based systems supporting more widespread networks based on Web servers. Such Internet-based systems offer excellent alternatives for HIEs and the NHIN, offering more accessible clients, better collaboration tools, and an expressive format for linking users together.

Complications crop up when considering the open Web system as a replacement for a closed system environment. At the very minimum, there is an open-systems integration challenge of replacing the old monolithic username/password database with a secure authentication environment in an open system.

The real benefits accrue as the web of trust expands outward from one organization to encompass the multiple organizations of even one HIE.. With the malleability of digital media (such as video, photographs, and even whole Web sites vulnerable to hacking), most authors on the subject state that digitally signed assertions of identity will become the standard.

For most applications that require strong authentication, PKI-based authentication provides the most secure means to meet all requirements.

A **public key infrastructure** (**PKI**) is an arrangement that binds public keys with respective user identities by means of a certificate authority (**CA**). The user identity must be unique for each CA. This is carried out by software at a CA, possibly under human supervision, together with other coordinated software at distributed locations. For each user, the user identity, the public key, their binding, validity conditions and other attributes are made un-forgeable in public key certificates issued by the CA. PKI arrangements enable computer users without prior contact to be authenticated to each other, and to use the public key information in their public key certificates to encrypt messages to each other . In general, a PKI consists of client software, server software, hardware (e.g., smart cards), legal contracts and assurances and operational procedures. A signer's public key certificate may also be used by a third-party to verify the digital signature of a message, which was made using the signer's private key.[22]

Over the past four years, growth in the realm of trust management has almost been exponential. This growth has been largely enabled by the development of loosely coupled web services that allow the use of federated identity models exchanging identity using SAML, XML and Simple Object Access Protocol (SOAP). Prior to this, most attempts to resolve trust centered on homogenizing how developers should handle trust. This approach required high levels of symmetry among participating systems and applications and was generally not supported by most popular applications. This approach placed inappropriate security burdens on the average developer resulting in expensive, complex infrastructure, and difficult to deploy, hard to use implementations that were generally deployed by enterprises under duress. Recently this scene has changed dramatically. For instance, Microsoft now offers identity management and certificate lifecycle management capabilities as "out of the box" applications. Numerous other vendors offer similar capabilities. Competition and technical advances have decreased costs, complexity and difficulty of implementation while increasing user acceptance.

[21] Matt Blaze, et al, AT&T Labs - Research, The Role of Trust Management in Distributed Systems Security
[22] http://en.wikipedia.org/wiki/Public_key_infrastructure

6.2 The Federal Government Approach

The strongest binding of credentials to identity is provided by using (PKI) which is widely used in government, the banking industry, the aerospace industry and others. The federal government requires the use of PKI across all branches and for all purposes whenever any electronic data is exchanged or transferred. The biopharmaceutical industry has also begun to use PKI through its development of the SAFE initiative[23]. For many reasons, the healthcare industry has, to date, been slow to adopt.

The Office of Management and Budget issued M-04-04 on 16 Dec 2003 to supplement OMB Circular A-130, Management of Federal Information Resources, Appendix II, Implementation of the Government Paperwork Elimination Act (GPEA). M-04-04 is the federal government's recognition of the requirement to provide a means to establish confidence in user identities presented to an electronic system for authentication. This guidance is also used by many non-Government trust schemas as the definitive source of guidance on authentication. The guidance goes on to establish levels of authentication assurance for transactions based on:

- Risks
- Likelihood of occurrence.

M-04-04 also identifies four levels of identity assurance.

By using a series of impact assessments, as defined in Federal Information Processing Standard (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems", it is possible to define the level of identity verification required for specific activities. Table 1 presents an overview of the factors that NIST recommends for assessment of potential harm and impact related to authentication errors.

Categories of harm and impact include:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss or agency liability
- Harm to agency programs or public interests
- Unauthorized release of sensitive information
- Personal safety
- Civil or criminal violations.

Category	Low	Medium	High
Inconvenience, distress or damage to reputation or standing	At worst, limited, short-term inconvenience, distress or embarrassment to any party.	At worst, serious short term or limited long-term inconvenience, distress or damage to the standing or reputation of any party.	Severe or serious long-term inconvenience, distress or damage to the standing or reputation of any party (ordinarily reserved for situations with particularly severe effects or which affect many individuals).
Financial loss	At worst, an insignificant or inconsequential unrecoverable financial loss to any party, or at worst, an insignificant or inconsequential agency liability.	At worst, a serious unrecoverable financial loss to any party, or a serious agency liability.	Severe or catastrophic unrecoverable financial loss to any party; or severe or catastrophic agency liability.
Harm to agency programs or public interests	At worst, a limited adverse effect on organizational operations or assets, or public	At worst, a serious adverse effect on organizational operations or assets, or public	A severe or catastrophic adverse effect on organizational operations or

[23] www.safe-biopharma.org

Category	Low	Medium	High
	interests. Examples of limited adverse effects are: (i) mission capability degradation to the extent and duration that the organization is able to perform its primary functions with *noticeably* reduced effectiveness, or (ii) minor damage to organizational assets or public interests.	interests. Examples of serious adverse effects are: (i) significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with *significantly* reduced effectiveness; or (ii) significant damage to organizational assets or public interests.	assets, or public interests. Examples of severe or catastrophic effects are: (i) severe mission capability degradation or loss of to the extent and duration that the organization is unable to perform one or more of its primary functions; or (ii) major damage to organizational assets or public interests.
Unauthorized release of sensitive information	At worst, a limited release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a low impact as defined in FIPS PUB 199.	At worst, a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a moderate impact as defined in FIPS PUB 199.	A release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a high impact as defined in FIPS PUB 199.
Personal safety	At worst, minor injury not requiring medical treatment.	At worst, moderate risk of minor injury or limited risk of injury requiring medical treatment	A risk of serious injury or death
Civil or criminal violations	At worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts.	At worst, a risk of civil or criminal violations that may be subject to enforcement efforts.	A risk of civil or criminal violations that are of special importance to enforcement programs.

Table 1 Determining Potential Impact of Authentication Errors[24]

Using the results of impact assessment using the factors in FIPS 199, OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies establishes four levels of identity verification. These are:

- Level 1: little or no confidence in the asserted identity's validity;
- Level 2: some confidence in the asserted identity's validity;
- Level 3: high confidence in the asserted identity's validity;
- Level 4: very high confidence in the asserted identity's validity.

M-04-04 goes on to identify a means to determine which level of verification should be required based on an assessment of the risks involved in activities that could derive from a loss of trust due to fallacious identities. Authentication errors with potentially worse consequences require higher levels of assurance. The risk from an authentication error is a function of two factors: potential harm or impact, and the *likelihood* of such harm or impact.

[24] Table derived from OMB, M04-04, E-Authentication Guidance for Federal Agencies, pgs 6 & 7

The following table from OMB M-04-04[25] provides an overview of the potential requirements:

Assurance Level Impact Profiles				
Potential Impact Categories for Authentication Errors	1	2	3	4
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

Table 2 Assurance Level Determination

The critical factor when discussing identity proofing is that only with a PKI-based solution is the credential used bound securely enough to the identity to provide strong assurance that the identity asserted is, in fact, that of the asserting party.

The federal government has established FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors to "achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to Federally controlled government facilities and electronic access to government information systems."[26]

A growing number of industry-based organizations have recognized the need to develop systems of trust and either have developed, or are in the process of developing, schemas which will provide requisite levels of trust for industry applications. Among the industries included are the aforementioned biopharmaceutical industry, the aerospace industry, the financial industry, the education industry and others.

Note that for any activity related to electronic medical records (EHR) and HIPAA, one may arrive at a requirement for at least a Level 2, more likely Level 3, identity verification.

6.2.1 The Federal Bridge Certification Authority

A common framework and infrastructure for future HIE digital identity may be found within the Federal Bridge Certification Authority (FBCA). The FBCA (fpkia.gsa.gov) is an information system that facilitates the entity-level acceptance of digital identity certificates issued by another entity for transactions. The FBCA functions as a non-hierarchical hub allowing the "relying party" entity to create a certificate trust path from its domain back to the domain of the entity that issued the certificate.[27]

The FBCA was originally started to facilitate disparate government agencies to communicate over a trust network that is mutually accepted. Practically, the FBCA itself is a certification Authority, however it does not issues certificates to users, it actually certifies other Certification Authorities, and is then certified by

[25] Ibid, pg 7
[26] FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors
[27] Federal Bridge Certification Authority. http://fpkia.gsa.gov

them in return in a processed known as “cross-certification.” This cross-certification generally takes place in three steps:

1. The FBCA and an applying entity review each others certification policies for compatibility;
2. The FBCA then issues a certificate to the applying entity; and finally
3. The applying entity issues a certificate back to the FBCA.

This cross-certification allows for paths of trust to be built between different agencies regardless of which individual entities are involved in the chain of information sharing. This process of cross-certification has allowed for a number of federal agencies (Department of Defense, Homeland Security, Energy, State, Treasury Justice, NASA, the Drug Enforcement Agency, Individual States, etc), as well as non government entities (such as Wells Fargo, ACES program, etc) and other bridges, like Certipath, to all connect and share a common proven system of trust.

This system of cross-certification could prove useful to HIEs as it enables digital transactions protected by two-factor authentication systems, digital signatures and strong encryption processes. This bridge model would allow for transactions to be trusted between different organizations, be it HIE and a Government Agency, between HIEs or between an HIE and a patient participating in that HIE.

HIEs could obtain certificates from FBCA authorized certification authorities such as those available under the GSA ACES program, or the Shared Service Provider Program which has certified entities like Exostar, a defense industry contractor and CyberTrust.

6.3 How do other industries manage?

The Financial Industry

The financial services industry relies heavily on PKI.

Anyone who has recently applied to open a bank account or get a debit card will recognize how authentication is performed in the financial industry. Typically, the bank officer requested to see at least one form of identification with a picture on it, and asked for at least one other form of identity that may have verified address or some other feature of a person’s identity. This process, known in the financial industry as “know your customer”, is very similar to the identity authentication (I&A) process used in most identity management schemes. The bank verifies identity and tightly couples that identity to an account and any activities related to that account.

For example, in applying for a debit card, the bank sends the card to the address provided during the application process in a plain white envelope. Once received, activating the card typically requires calling an 800 number from a home phone (another piece of personal information provided during the application process). The system captures the number of the caller and compares it to the number recorded in the account information. If it matches, the automated response system asks for the card number and then will typically ask the recipient to perform another action, e.g. enter the expiration date on the front of the card. This is a process that verifies that the intended recipient has in fact received the card, i.e., the identity token. This is the first factor that will be used to access a bank account from an ATM machine (referred to earlier as “something you have”).

This one factor is not sufficient for the bank to release money to the card holder. Possession of the card at the machine is not a strong enough means of authentication. The PIN number, usually a 4 to 10 digit number known only to the card holder and the automated system at that bank, serves as the second authentication factor (referred to earlier as “something you know”).

This example is just one instance of how the financial services industry manages identity and maintains trust across its myriad systems. Mortgage processing, funds transfer, investment management – all these applications require strong trust and are supported by public key infrastructure. In fact, the financial services industry was the first to broadly move to PKI.

The Biopharmaceutical Industry

The biopharmaceutical industry realized in 2003 that it was facing growing costs and regulatory pressures in its core business area – research and development. The industry was almost totally paper-based and was spending over $40B annually managing paper. At the same time there was increasing pressure to move to a more collaborative means of developing and managing drugs. R&D costs were skyrocketing and the time to bring a new drug to market was increasing rapidly. The requirement for more and more clinical trials mandated an increased number of relationships with clinical investigators. Companies also began to out-source some parts of the development process, e.g., clinical trial management, data management, conduct of pre-clinical trials, etc. The costs for managing an ever-increasing number of contracts and the need to verify identities of all the participants were growing. At the same time, requirements for security, intellectual property and data protection were becoming more stringent.

Regulatory agencies were beginning to mandate the submission of electronic files instead of the traditional paper. This regulatory requirement added to the need to ensure that signatures on these files were tightly coupled to the individual who signed them, were difficult to repudiate and that somehow the integrity of the data that was signed was maintained, or that any tampering with the files after signature was readily evident.

All these factors drove the world's largest biopharmaceutical companies to seek alternatives. In 2005 the search led to the development of the Signatures and Authentication for Everyone (SAFE) Standard to manage identities and use digital signatures for "business to regulator" and "business to business" documents. In mid-2005 the industry created the SAFE-BioPharma Association to manage the continued development and maintenance of the SAFE digital identity and signature standard. There were a number of objectives for this initiative, including:

- Identity management that would lead to one form of identity for any participant in the system. Clinical investigators often work with more than one pharma on clinical trials. Each pharma would verify the investigator's identity using many different processes and would then provide the investigator with a user name and password to access the pharma's infrastructure. The result was multiple user names and passwords --one identity for each pharma with whom they worked. They used sticky notes attached to each pharma system with the user name and password available for anyone to use. The industry developed as part of the SAFE Standard provides the means to verify the investigator's identity and strongly tie the identity to the individual. This single identity would be used by all industry companies that were members of SAFE. In addition to one form of identity for each user, SAFE provides multiple levels of assurance based on the requirements of the supported business process. For some requirements for system authentication, a basic assurance level would be sufficient. For other processes that require the application of digital signatures, a higher medium level of assurance is required. SAFE can support each of these using the same infrastructure.
- Support for a high level of non-repudiation. The SAFE Standard achieves this by virtue of its subscriber agreement and the use of identity tokens. The user of the token agrees by formal contract to abide by the SAFE rules for use and further agrees that every time they use their digital identity to sign a document they agree that the signature will be covered under the SAFE Standard, and that they intend this to be their legally binding signature. If they fail to abide by their subscriber agreement and, for instance, give the pass phrase associated with their token to someone else to use to apply signatures to documents or authenticate to a system, they face severe financial penalties and revocation of their credential.
- Support for strong document/data integrity. SAFE is a PKI-based system. When a digital signature is applied to a document, a cryptographic operation is applied that in essence certifies the document. When the signature is verified, another cryptographic operation verifies not only the validity of the certificate used to apply the signature, but also will verify that the document has not been changed (not even a single byte is different) since it was signed.

The industry looked at many alternatives and settled on PKI as the most appropriate technology to meet the many different requirements it faced. The SAFE Bridge certification Authority is in the process of cross certifying with the Federal Bridge.

The Defense and Aviation Industry

The federal government, as noted, has established guidance supporting identity management, system authentication and other aspects related to establishing a system of trust. In response to actions by the Government and to support increasing requirements for interaction and interoperability, major players in the industry including Boeing, Northrop Grumman, Lockheed Martin, Raytheon, BAE Systems, EDS and the U.S. Government backed an effort begun by ARINC, EXOSTAR and SITA to "design, implement, maintain and market a secure public key infrastructure communications bridge, initially focused on the aerospace and defense industry. This enables the transfer of secured and authenticated information globally between subscribing companies; and between such companies and a number of domestic and foreign government agencies."[28]

The initial concept of an "Aerospace & Defense Bridge" was driven by the UK MoD, US DoD, aerospace/defense industry and exchanges to meet collaborative business goals that require information to be shared more widely, securely, effectively and affordably between the U.S., U.K. and other European nations. This idea was predicated on the wide acceptance of PKI (Public Key Infrastructure) based credentials being the best credential technology available.

To meet this identified need, CertiPath was formed in June 2005 to provide identify assurance services, by operating a PKI bridge and cross-certifying enterprises onto this bridge"[29]

CertiPath is cross certified with the Federal Bridge Certification Authority and provides the following services using PKI. These services will allow users of the CertiPath bridge to perform the following business tasks with anyone else who is part of the Bridge:

- Secure document exchange;
- Collaborative engineering;
- Secure e-mail;
- Digital Signatures/non-repudiation of transactions;
- Transaction security between systems.

7. Public Key Infrastructure

Public key infrastructure (PKI) provides organizations a means to strongly control identities and support strong authentication and identity verification. In addition, PKI provides other benefits, ***especially when based on open technology architectures***. PKI has existed for some time but has been viewed, until recent technological and policy advancements, as too hard and too expensive to implement. In a recent response to a Wall Street Journal article of July 3, 2007 entitled "Signing up for E-Signatures", Peter Hesse, President of Gemini Security Solutions, Inc wrote:

> "Much fuss has been made about the difficulty of managing a PKI, certificates, and smart cards. The last seven years has brought great strides in the simplicity and commoditization of security technologies such as PKI. Modern operating systems (Windows, OSX, etc.) all come with PKI support throughout the desktop — PKI is used behind the scenes to validate signed executables, secure websites, etc. Applications such as Microsoft Office, Adobe Acrobat, and many others come with support for PKI-based digital signatures and encryption. While PKI technology can be used for authentication, signatures/approvals, and confidentiality, E-Signatures only provide a solution for signatures/approvals. A PKI can enable organizations to replace all passwords with certificate-based authentication, and provide the capability to perform persistent digital signature and strong encryption. The cost savings in avoiding password resets alone can often provide a sufficient return

[28] http://www.certipath.com/about.htm, CertiPath Web Site, About Us
[29] Ibid.

on investment, and combining this with the advantages of using electronic workflows and documents instead of pushing paper, makes clear the value of PKI."[30]

As noted by Mr. Hesse, PKI (digital identities included) support is becoming more ubiquitous across platforms and operating systems and is being used for activities noted without users even being aware. The open standards for technology and communication using PKI exist and are being expanded on a rapidly increasing basis. This allows architects and integrators the ability to provide much stronger capabilities to implementing agencies and organizations. The use of standards such as Security Assertion Markup Language (SAML) to provide authentication enhances interoperability.

Much has been said about problems of scalability in the use of PKI - certificate form factors are restrictive, identity verification is cumbersome and hard to do, implementation of PKI is costly and technically difficult, etc. Many of these comments are based on old information and practices. As with any technology, as time passes major improvements are made and it is critical to stay current with the facts. Increasing need for security and protection of identity and data points to increasing requirements for the benefits of PKI-based solutions. The federal government has recognized this need and has established the Federal Bridge Certification Authority to support e-business with the Government. The National Institute for Standards and Technology has made major investments in, and has developed numerous open standards to support, PKI. So what has changed to make PKI more attractive and useful? The following sections provide some high level information that is expanded in Appendix B.

Token Form Factors

Digital identity credentials reside and are protected by tokens. Tokens exist in a number of different forms. Form factors include: hardware tokens, smart cards, network hosted certificates, software certificates and soon, USB3 tokens. Each has benefits and drawbacks. The key is that there are now different technologies. We discussed in a subsequent section NIST recommendations for token use. It is noteworthy that even the NIST recommendations are somewhat dated since they do not include discussion of network hosted certificates or USB3 tokens due to the difficulty of maintaining pace with the advance of technology. However, we note that NIST has advised that it is in the process of revising NIST SP 800-63 to account for changes and advances in technology. The fact is that use of different types of tokens may be determined by the using organization based on risk and use requirements as long as the certificate policy of the issuing CA accepts the form. The development of different forms of tokens occurred specifically because of issues related to scalability and use of the original forms. It is no longer necessary to download drivers or carry around smart card readers to use digital certificates. There are viable options.

7.1 Implementation Costs

Early implementers faced a number of issues in implementing PKI, many of which related to cost and technical infrastructure. In the early days of PKI there were few, if any, third parties that would provide PKI services as an outsourced option. Therefore, early adopters had to develop internal infrastructures that were expensive and technically complex. While the development of internal infrastructures to support PKI is still an option, there are now a growing number of third parties that provide PKI services as an outsourced service at reasonable costs. For those organizations that determine an internal infrastructure best meets their needs, the costs have declined significantly and continue to decline with the development of new technologies.

As recently as four years ago it could cost a mid-sized company in the vicinity of $15 million to establish and operate an enterprise-wide PKI. The high costs were exacerbated by the fact that there were no established standards for development and operation so an implementing organization would have to establish its own standard, based on best practice. Cross certification and scalability were further

[30] Peter Hesse letter, http://www.securitymusings.com, July 4, 2007.

impacted by this fact since the time and effort to ensure certificate policies mapped and trust could be established to allow interoperability were significant.

In the past few years NIST has developed FIPS standards that govern PKI. These standards support significantly improved commonality and interoperability among commercially available PKI components. The use of proprietary products and software has been greatly reduced. More commercial offerings are available and competition has had a positive effect on pricing. Current experience supports PKI roll-out for a small-to-mid size biotechnology firm using Microsoft Certificate Services and Certificate Lifecycle Manager with supporting hardware and full FDA system validation in the lower end of a range of $250-500,000. As previously noted, with the growth in the use of PKI, has made it economically feasible for third party providers to offer PKI-based identity and digital certificate management services on a contract basis. This means that PKI-based capability now is available to nearly any organization that needs strong assurance.

7.2 Authentication to Systems

Digital identities managed in a PKI can be used to authenticate to organizational systems and infrastructure, eliminating the need for user names and passwords thereby providing significant savings in infrastructure costs related to user name and password management. More detailed information is included in Appendix B.

7.3 Authorization

Authentication to a system is only the first step in gaining access to data. Authorization is the process of granting properly authenticated users access to data and in many cases, permissions to take specific actions related to those data, e.g., create, change, revise, view, delete, etc. Authorization is controlled by the internal administrators of systems in an enterprise infrastructure and is outside the scope of this paper.

7.4 Digital Signatures

A digital signature tightly binds the identity of the signer to the contents of the data that is signed. This fact provides strengthened non-repudiation of the signature at a later date. The digital signature creation and verification process also provides relying parties assurance that the integrity of the signed document has not been compromised since the document was signed. The following discussion provides the basis for the preceding statements. Although this discussion relates to SAFE digital signatures, the process is basically the same for any digital signature. The information presented below was extracted form the SAFE Digital Signature Use and Verification Process Guideline.

Most organizations using digital signatures require some level of acknowledgment that the signing party knows the signature they are about to apply is the legally binding equivalent of their handwritten, ink signature. In most cases, this is accomplished when the signer applies their pass phrase to gain access to their private key.

7.5 Costs and Benefits Overview

The following table[31] provides a comparison among various technical means to manage identities in a PKI-based infrastructure. The table reviews options in terms of cost to implement and use, the benefits on a low to high scale of benefits provided and three primary applications – authentication to networks and facilities and use in e-commerce applications. It should be noted that the costs for infrastructure, especially for PKI-based solutions have come down significantly over the past few years to the point that a PKI solution can be implemented for well under $500,000 or may be contracted to a third party provider for even less.

Mediums/Technologies	Cost Factors			Benefits									Applications		
	Token	Reader	Infrastructure	Non-repudiation	Authentication - originator verification	Data Integrity	Confidentiality - privacy with encryption	Scalability - ability to add applications	Portability - ease of transport	Interoperability - ability to share data	Efficiency - productivity via automation	Data storage capacity	Logical Access- network access	Physical access - building access[32]	e_commerce - stored value
Bar Code Card	$	$$	$	L	L	L	L	L	H	H	M	L	N	Y	N
Magnetic Stripe Card	$	$$$	$	L	L	L	L	L	H	H	M	L	N	Y	Y
User ID/Password	NA	NA	$	L	M	M	L	L	H	L	L	NA	Y	Y	N
PKI -software	NA	NA	$$$	H	H	H	H	M	L	M/H	H	NA	Y	N	Y
PKI Hardware token/smart card	$$	$$	$$$	H	H	H	H	H	H	M/H	H	H	Y	Y	Y
PKI Network based	NA	NA	$$$	H	H	H	H	H	H	M/H	H	H	Y	N	Y
PKI H/W token w biometrics	$$	$$$	$$$	H	H	H	H	H	H	M/H	H	H	Y	Y	Y

Token	Readers		
$ = $.10 - 5.00	$ = <$50.00	High	Yes
$= $5-10.00	$$ = $50-100.00	Medium	No
$$$= >$10.00	$$$ = > $100	Low	

Table 3 Technology Comparison

[31] SAFE-BioPharma Assn
[32] Government standards advocate the use of an attended biometric process for building access.

Table 2 looks at relative costs and benefits that derive from different token types in a PKI-based solution. It includes the types of tokens that support three of the most commonly used levels of assurance as developed by the federal government. Cost figures in this table are relatively the same as in Table 1 except that costs for infrastructure are relative to each other.

Assurance Level		Costs				Benefits								Usage				
		Support	Readers/Devices	Infrastructure	I & A Requirements	Non-repudiation	Data Integrity	Confidentiality	Portability	Regulatory Compliance (Global)	Scalability (low impact on desktop)	Adoptability	Security Assurance	Authentication	Encryption	Logical Access	Physical Access	Digital Signatures
Low	Machine Stored Software certs	$	$	$														
Medium	Machine Stored Software Certs	$	$	$														
	Remote Hosted HSM certs	$	$$	$$														
Medium Hardware	USB Token	$$	$$	$$														
	Smart Card	$$	$$	$$														
	Biometric	$$	$$$	$$$														
	USB3	$		$$														

Low or Not Existent
Moderate
High

Table 4 Token Comparison[33]

[33] SAFE-BioPharma Assn

8. Findings and Recommendations

8.1 Findings

Findings

- HIE has the potential to significantly improve the quality of healthcare, and therefore the health, of the American populace;
- HIE, to be truly successful, requires the application of consistent standards and policies that can work in harmony across state boundaries, including policies for digital identity management;
- Technology continues to evolve, both in identity management and data systems interoperability. As these technologies evolve, health information exchange initiatives will have to maintain awareness of this evolution and can take advantage of these advances.
- Digital identities that are tightly bound to the individual provider offer significant benefits, especially in terms of trust assurance and security, in processes involving authentication to systems outside of a user's parent organization;
- The development of a nationwide network of trust, predicated on strong identity management, is critical to moving HIE forward;
- There are existing models for the development of networks of trust that bear understanding and either implementation or modification to meet HIE needs. It is not necessary to reinvent the wheel.

8.2 Recommendations

General Recommendations:

- Awareness of identity management and the need for standard policies and interoperability should be expanded across national public and private sector initiatives, as well as the HIE community;
- Policies and procedures for identity management in HIEs should be further explored and tested in 2008, and lessons learned should be reported to the HIE community.
- To support and foster interoperability, the rules implemented as part of the Federal Common Policy should inform the identity management policies of HIEs.

Members of the SAFE-Biopharma community make the following specific recommendations to HIEs. These recommendations are based on their experience in exchanging sensitive clinical research and other proprietary data between companies, regulators, clinicians and others:

- Form trust networks through a system of closed contracts. The use of a closed contract model provides safeguards by removing enforcement from state or other jurisdictional law, and places it under contract law. It binds members to approved policies and procedures, allows arbitrated dispute resolution, provides the ability to set liability limits and eliminates cumbersome bilateral agreements. This will help address potential issues when HIEs begin to interact with other HIEs as part of a nationwide health information network (NHIN) and provides a common set of policies and guidelines for identity management.
- Develop common policies, procedures and guidelines in order to bind users to them through contracts. The common policies and guidelines developed in closed contract models provide a standard method to manage the life cycle of a digital identity, with specific responsibilities levied on actors in the system at various points. This provides the means to enforce specific actions

and consequences for failure to adhere to the rule set. It also provides clear and unequivocal guidelines to all actors for the use of digital identities managed within the system.

- Separate authentication and authorization. Authentication confirms, asserts and validates an identity as being the individual, while authorization grants specific rights based on authenticated identity.
- Authenticate as an individual (vs. organization or role), and authorize based on role. There are a number of ways to implement this recommendation that should be investigated. Roles in digital certificates may present issues in the life cycle management of such credentials that impact the users, especially if their role changes.
- Consider cross-certification with Federal Bridge CA as part of the architecture for NHIN identity management. This would provide interoperability with federal agencies, and potentially provide a platform for use by all networks participating in the NHIN.

9.0 About SAFE-BioPharma Association

SAFE-BioPharma Association (Signatures and Authentication for Everyone) is a non-profit biopharmaceutical industry association created by the world's leading biopharmaceutical companies. SAFE™ was established to develop and maintain an industry identity management and digital signature standard to permit highly regulated pharma companies to shift to fully electronic business-to-business and business-to-regulator processes by providing a recognized industry-wide identity management standard and legally enforceable and regulatory-compliant digital signatures.

The SAFE standard is now being implemented by association member companies in a variety of applications. The standard continues to change and evolve based on experience gained in its use. The biopharmaceutical industry includes clinical investigators and other healthcare professionals and seeks to interoperate with the broader healthcare community as it implements HIT and adopts identity management and digital signatures standards.

SAFE is partnering, under a contract with eHI, to explore and raise awareness of identity management and digital signature issues with the broader health community.

10.0 About the eHealth Initiative

The eHealth Initiative and its Foundation are independent, non-profit affiliated organizations whose missions are the same: to drive improvements in the quality, safety, and efficiency of healthcare through information and information technology.

eHI engages multiple stakeholders, including clinicians, consumer and patient groups, employers, health plans, health IT suppliers, hospitals and other providers, laboratories, pharmaceutical and medical device manufacturers, pharmacies, public health, public sector agencies, and its growing coalition of more than 200 state, regional and community-based collaboratives, to reach agreement on and drive the adoption of common principles, policies and best practices for improving the quality, safety and effectiveness of healthcare through information and information technology. For more information, go to www.ehealthinitiative.org.

Appendix A - Health Information Exchange Identity Management.

In the existing and proposed HIEs, several approaches to identity management are being undertaken.

It is difficult, at best, for any given HIE to function at the required levels of security and regulatory compliance without a standard method of identity management across its membership. If all members of the HIE are not operating under a standard methodology it is impossible for the HIE to verify identities and allow access to data across different HIEs. As noted in the previous discussions of identity verification and authentication, participating organizations must perform identity verification to the cited levels of compliance with Federal standards. This can be accomplished with minimal impact on both organizations and individuals and can be scaled to support most any type of organization from a large hospital to a small private practice.

The following discussion describes an approach which could be readily modified or adapted to support the issuance of PKI based digital identity certificates:

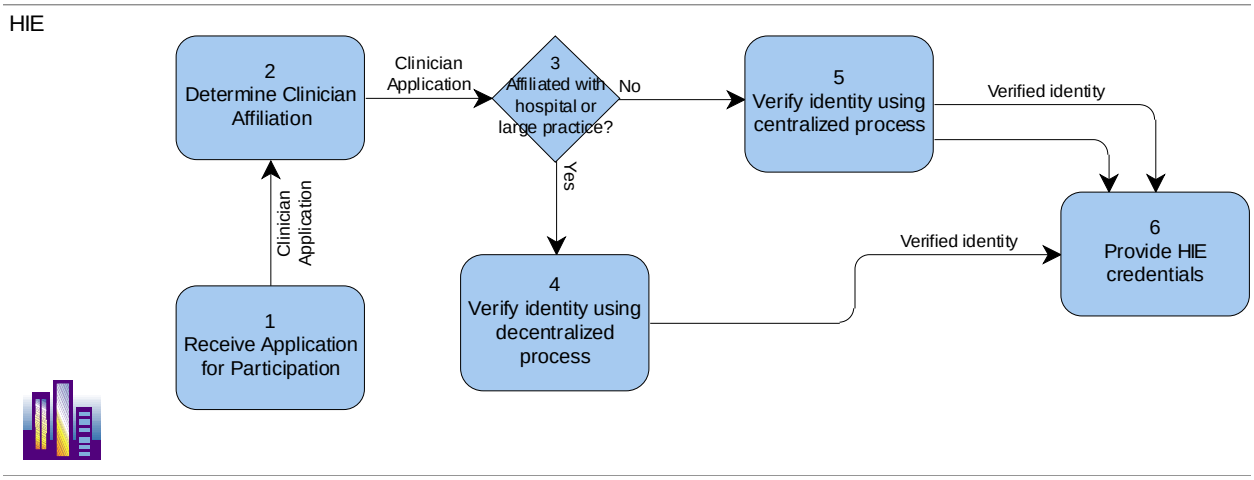

Figure 2 Clinician Credentialing

Organization: HIE

A Health Information Exchange is an organization created to support the mobilization of healthcare information electronically across organizations within a region or community.

An HIE provides the capability to electronically move clinical information between disparate healthcare information systems while maintaining the meaning of the information being exchanged. The goal of the HIE is to facilitate access to and retrieval of clinical data to provide safer, more timely, efficient, effective, equitable, patient-centered care.

Organization: Affiliated Hospital or Practice

These are organizations that are affiliated with the HIE as members.

Step 1: Receive Application for Participation

This step is the responsibility of the HIE.

The HIE receives an application for clinician participation from the sponsoring organization which may be a participating hospital, a large clinic or a small private practice.

Output:

- Clinician Application to Activity: 2 Determine Clinician Affiliation

Step 2: Determine Clinician Affiliation

This step is the responsibility of the HIE.

Upon identification of a clinician who desires to participate in the Electronic Health Information Exchange, the affiliation of the clinician is first derived. Clinicians may be affiliated via employment or through the granting of privileges with a hospital or other health delivery organization, e.g., large clinical practice, which verifies the identity of the clinician using face to face means that requires the presentation of one or more forms of identity that either verify the individuals eligibility to work in the United States (known as the I-9 process) or by some other means verify with certainty that the individual is who they purport to be. In all cases, the organization maintains copies of the materials used to prove identity for audit and legal requirements.

Input:

- Clinician Application from Activity: 1 Receive Application for Participation

Output:

- Clinician Application to Activity: 5 Verify identity using centralized process based upon a No condition for Decision Point: 3 Affiliated with hospital or large practice?
- Clinician Application to Activity: 4 Verify identity using decentralized process based upon a Yes condition for Decision Point: 3 Affiliated with hospital or large practice?

Step 3: Determine Affiliation with hospital or large practice

This step is the responsibility of the HIE.

Step 4: Verify identity using decentralized process

This step is the responsibility of the HIE.

In the case of a clinician affiliated with a hospital or large clinic as an employee or with privileges, the HIE uses a decentralized process that relies on the affiliated organization's identity verification procedures.

Input:

- Clinician Application from Activity: 2 Determine Clinician Affiliation based upon a Yes condition for Decision Point: 3 Affiliated with hospital or large practice?

Output:

- Verified identity to Activity: 6 Provide HIE credential

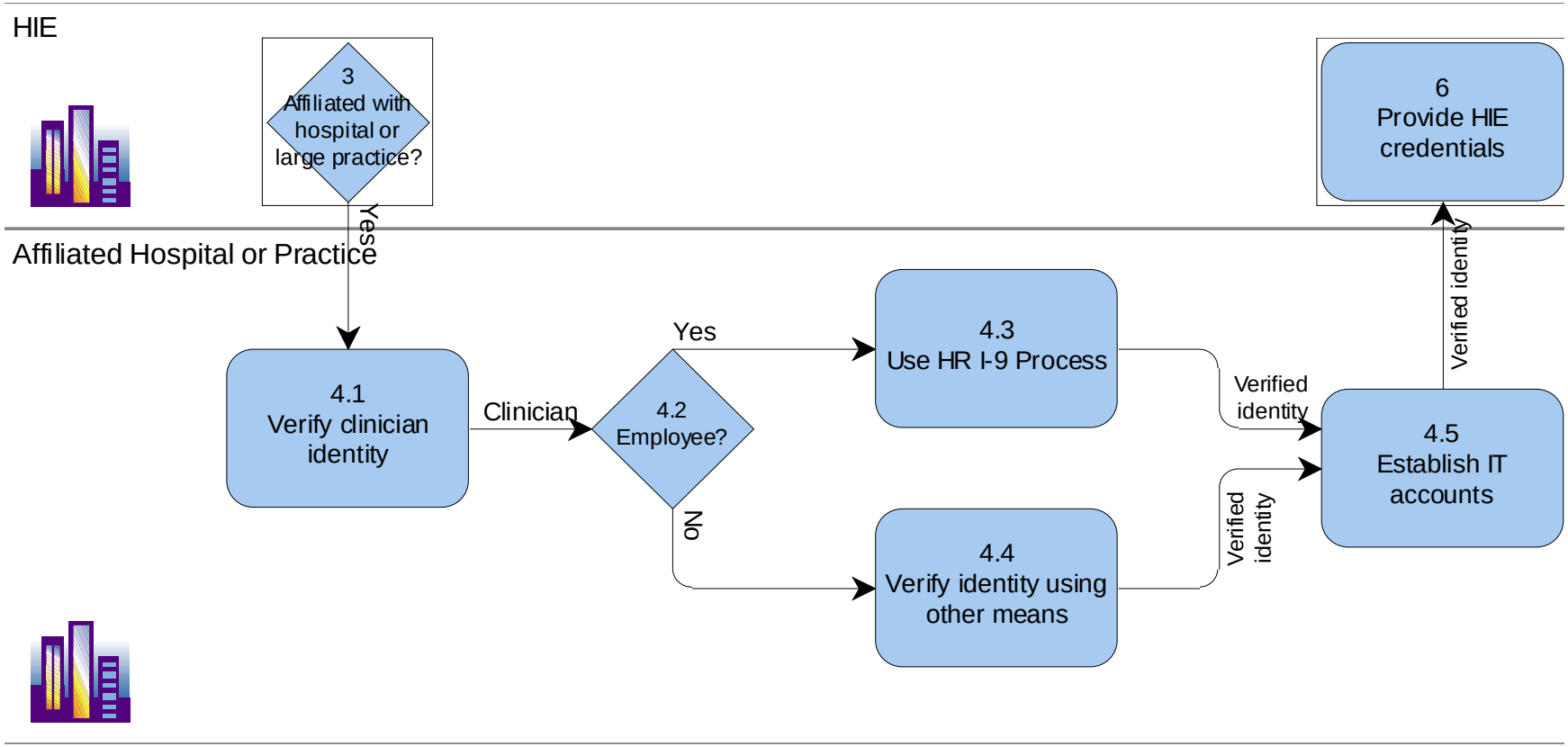

Figure 3 Distributed Approach Identity Authentication

Step 4.1: Verify clinician identity

This step the responsibility of the Affiliated Hospital or Practice.

The hospital or practice verifies the clinician's identity as part of the employment or granting of privileges process.

Input:

- Workflow from Decision Point: 3 Affiliated with hospital or large practice? Based upon a Yes condition for Decision Point: 3 Affiliated with hospital or large practice?

Output:

- Clinician to Activity: 4.4 Verify identity using other means based upon a No condition for Decision Point: 4.2 Employee?
- Clinician to Activity: 4.3 Use HR I-9 Process based upon a Yes condition for Decision Point: 4.2 Employee?

Step 4.2: Determine if the Clinician is an Employee

This step is the responsibility of the Affiliated Hospital or Practice.

Step 4.3: Use Human Resources I-9 Process

This step the responsibility of the Affiliated Hospital or Practice.

In all cases of determining an individual eligibility to work within the U.S., Human Resources departments are required to review identity documents that establish either U.S. citizenship or an authorized visa that establishes the individual's eligibility to work in the United Sates. There are very specific forms of identification that must be presented, at least one of which usually requires a picture ID. Copies of the documentation must be made and maintained by the HR department. Based on successfully proving the eligibility to work in the U.S., the HR department may issue an organizational form of identification to the clinician.

Input:

- Clinician from Activity: 4.1 Verify clinician identity based upon a Yes condition for Decision Point: 4.2 Employee?

Output:

- Verified identity to Activity: 4.5 Establish IT accounts

Step 4.4: Verify identity using other means

This step is the responsibility of the Affiliated Hospital or Practice.

Since the clinician is not an employee, the organization must use other means to verify their identity. These means may include verifying the clinician's professional license which may or may not also include verifying their identity using such means as a passport, driver’s license, etc, which have a picture to verify the identity in a face to face meeting. In most states, the professional licensing process also requires face to face identity verification and maintenance by some department within the hospital or clinic of copies of the forms of identity used to verify the identity.

Input:

- Clinician from Activity: 4.1 Verify clinician identity based upon a No condition for Decision Point: 4.2 Employee?

Output:

- Verified identity to Activity: 4.5 Establish IT accounts

Step 4.5: Establish IT accounts

This step is the responsibility of the Affiliated Hospital or Practice.

Based on the verified identity of the clinician the IT department creates user names and passwords (or other credentials) and establishes permissions/authorization for the clinician to access IT resources needed to perform their role in the organization.

Input:

- Verified identity from Activity: 4.3 Use HR I-9 Process
- Verified identity from Activity: 4.4 Verify identity using other means

Output:

- Verified identity to Activity: 6 Provide HIE credentials

Step 5: Verify identity using centralized process

This step is the responsibility of the HIE.

In the case of clinicians at smaller practices or those not affiliated with hospitals or other larger clinics, the HIE uses its centralized identity verification process.

Input:

- Clinician Application from Activity: 2 Determine Clinician Affiliation based upon a No condition for Decision Point: 3 Affiliated with hospital or large practice?

Output:

- Workflow to Activity: 6 Provide HIE credentials
- Verified identity to Activity: 6 Provide HIE credentials

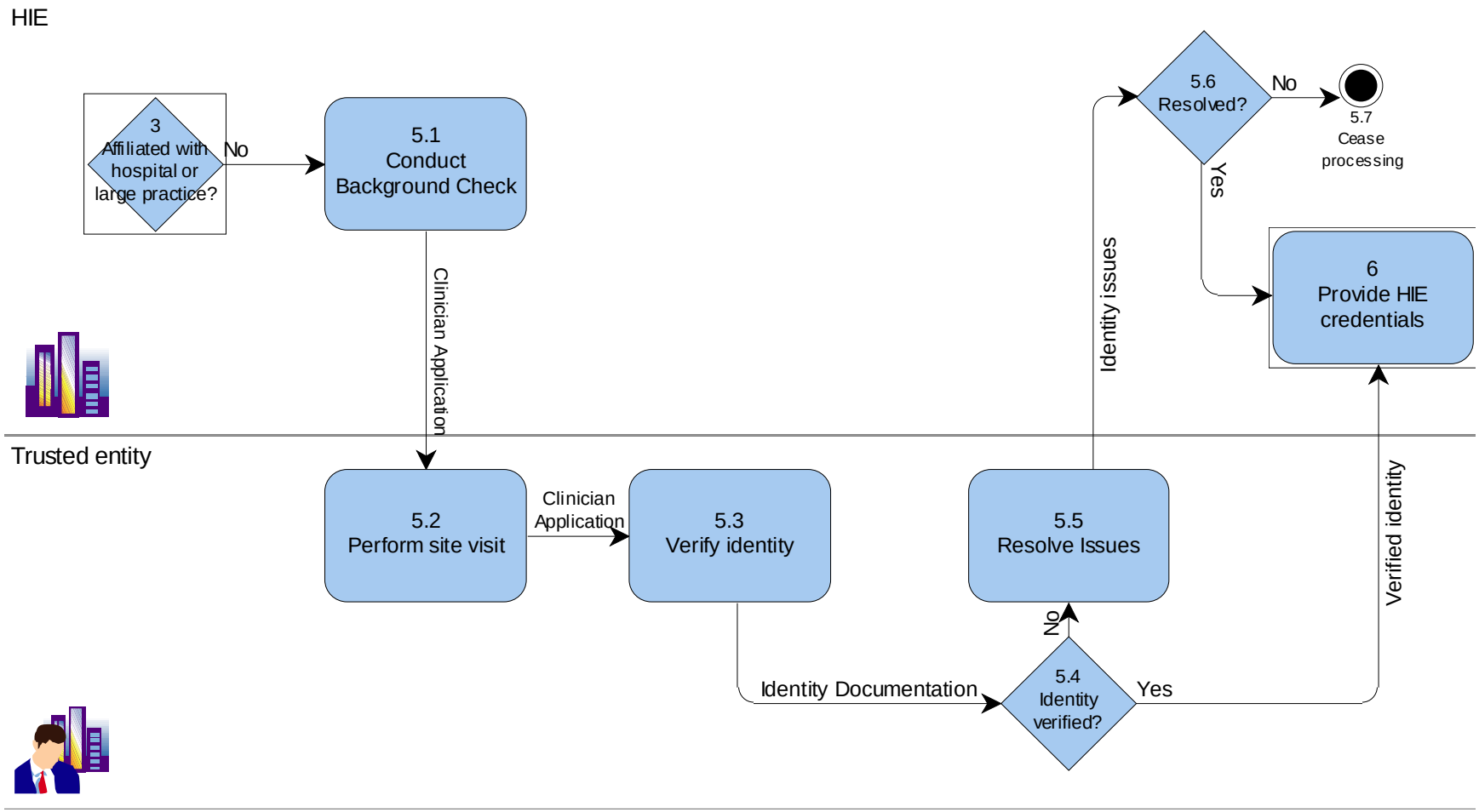

Figure 4 Centralized Approach Identity Authentication

Role: Trusted entity

This is an individual who is designated by the HIE to perform identity authentication of applicants for HIE credentials. The individual may be an employee of the HIE, a contracted individual or some other entity acting under written authorization from the HIE to perform the identity authentication using written standards for performance.

Step 5.1: Conduct Background Check

This step is the responsibility of the HIE.

Input:

- Workflow from Decision Point: 3 Affiliated with hospital or large practice? based upon a No condition for Decision Point: 3 Affiliated with hospital or large practice?

Output:

- Clinician Application to Activity: 5.2 Perform site visit

Step 5.2: Perform site visit

This step is the responsibility of the Trusted entity.

The HIE sends its representative to the site to review the site and also conduct a face to face identity authentication acting as the trusted agent of the HIE.

Input:

- Clinician Application from Activity: 5.1 Conduct Background Check

Output:

- Clinician Application to Activity: 5.3 Verify identity

Step 5.3: Verify identity

This step is the responsibility of the Trusted entity.

The HIE trusted entity verifies the identity of the clinician using approved forms of ID and also reviews the professional license to ensure currency and accuracy if the information.

Input:

- Clinician Application from Activity: 5.2 Perform site visit

Output:

- Identity Documentation to Activity: 5.5 Resolve Issues based upon a No condition for Decision Point: 5.4 Identity verified?
- Identity Documentation to Activity: 6 Provide HIE credentials (in the form of Verified identity) based upon a Yes condition for Decision Point: 5.4 Identity verified?

Step 5.4: Decision Point: Identity verified?

This step is the responsibility of the Trusted entity.

Step 5.5: Resolve Issues

This step is the responsibility of the Trusted entity.

The HIE trusted entity attempts to resolve any issues with the identity authentication.

Input:

- Identity Documentation from Activity: 5.3 Verify identity based upon a No condition for Decision Point: 5.4 Identity verified?

Output:

- Identity issues to Sink: 7 Cease processing based upon a No condition for Decision Point: 5.6 Resolved?
- Identity issues to Activity: 6 Provide HIE credentials based upon a Yes condition for Decision Point: 5.6 Resolved?

Step 5.6: Decision Point: Resolved?

This step is the responsibility of the HIE.

Step 5.7: Provide HIE credentials

This step is the responsibility of the HIE.

Based upon the authentication of the applicant identity, the HIE issues the appropriate credential to allow the clinician to participate in the network. The credential may be any of the types of credentials cited in this paper depending on the level of use by the HIE.

Input:

- Workflow from Activity: 5 Verify identity using centralized process
- Verified identity from Activity: 4 Verify identity using decentralized process
- Verified identity from Activity: 5 Verify identity using centralized process.

Appendix B – Public Key Infrastructure

Authentication to Systems

NIST SP 800-63 provides the following authentication guidance:

> **Level 1** - Although there is no identity proofing requirement at this level, the authentication mechanism provides some assurance that the same claimant is accessing the protected transaction or data. It allows a wide range of available authentication technologies to be employed and allows any of the token methods of Levels 2, 3 or 4. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token.

- **Level 2** – Level 2 provides single factor remote network authentication. At Level 2, identity proofing requirements are introduced, requiring presentation of identifying materials or information. A wide range of available authentication technologies can be employed at Level 2. It allows any of the token methods of Levels 3 or 4, as well as passwords and PINs. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. Eavesdropper, replay and on-line guessing attacks are prevented.

- **Level 3**- Level 3 provides multi-factor remote network authentication. At this level, identity proofing procedures require verification of identifying materials and information. Level 3 authentication is based on proof of possession of a key or a one-time password through a cryptographic protocol. Level 3 authentication requires cryptographic strength mechanisms that protect the primary authentication token (secret key, private key or onetime password) against compromise by the protocol threats including: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks. A minimum of two authentication factors is required. Three kinds of tokens may be used: "soft" cryptographic tokens, "hard" cryptographic tokens and "one-time password" device tokens.

- **Level 4 –** Level 4 is intended to provide the highest practical remote network authentication assurance. Level 4 authentication is based on proof of possession of a key through a cryptographic protocol. Level 4 is similar to Level 3 except that only "hard" cryptographic tokens are allowed, FIPS 140-2 cryptographic module validation requirements are strengthened, and subsequent critical data transfers must be authenticated via a key bound to the authentication process. The token shall be a hardware cryptographic module validated at FIPS 140-2 Level 2 or higher overall with at least FIPS 140-2 Level 3 physical security. By requiring a physical token, which cannot readily be copied and since FIPS 140-2 requires operator authentication at Level 2 and higher, this level ensures good, two factor remote authentication.

A system uses two-factor authentication when it requires at least two of the authentication form factors mentioned above. This significant difference from single-factor authentication greatly enhances security in authentication. Certainly individual health records and the information included therein, require the strong security protections afforded by two-factor authentication. Under the cited Federal PIV program, access to critical federal systems will require two-factor authentication. It is highly likely that access to many HHS systems, especially those that use the Federal Bridge, will require two-factor authentication.

SAFE operates a two-factor authentication scheme and the SAFE Bridge Certification Authority (SBCA) will soon be cross certified with the FBCA. Once cross-certification is complete, SAFE certificates will be able to be used to authenticate to sites served by the FBCA.

NIST SP 800-63 also provides guidance related to the types of tokens that should be used at different levels of authentication. SP 800-63 defines a token as : "Tokens generically are something the claimant possesses and controls that may be used to authenticate the claimant's identity."[34] SP 800-63 suggests four types of tokens as follows:

- Hard token – a hardware device that contains a protected cryptographic key.

  Authentication is accomplished by proving possession of the device and control of the key. Hard tokens shall:

  - Require the entry of a password or a biometric to activate the authentication key;
  - Not be able to export authentication keys;
  - Be FIPS 140-2 validated:
    - Overall validation at Level 2 or higher,
    - Physical security at Level 3 or higher.
- Soft token – a cryptographic key that is typically stored on disk or some other media. Authentication is accomplished by proving possession and control of the key. The soft token key shall be encrypted under a key derived from some activation data. Typically, this activation data will be a password known only to the user, so a password is required to activate the token. For soft tokens, the cryptographic module shall be validated at FIPS 140-2 Level 1 or higher, and may be either a hardware device or a software module.
- One-time password device token - a personal hardware device that generates "one time" passwords for use in authentication.
- Password token – a secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings, however some systems use a number of images that the subscriber memorizes and must identify when presented along with other similar images.

Finally, NIST SP 800-63 assigns the use of tokens to the four authentication levels as follows:

- Password tokens can satisfy the assurance requirements for Levels 1 and 2.
- Soft cryptographic tokens may be used at authentication assurance Levels 1 to 3, but must be combined with a password or biometric to achieve Level 3.
- One-time password devices are considered to satisfy the assurance requirements for Levels 1 through 3, and must be used with a password or biometric to achieve Level 3.

Digital Signatures

Creation of the Digital Signature

The signature creation process calculates and formats the Digital Signature. The signature is derived from and is unique to both the message and the signer's private key. Note that the "information to be signed" is the "message" in the signature creation sub-process described and illustrated below. The Digital Signature creation application must:

a. Hash the message content (i.e. the selected information) and any authenticated attributes to create the message digest. At a minimum, SAFE requires the use of the signing-time authenticated attribute.

b. Prompt for the SAFE credential pass-phrase to access the signature private key

c. Sign the message digest

d. Create a PKCS #7 or CMS (per RFC 3369) or XML DSig signature container

[34] NIST SP 800-63, Section 5.2

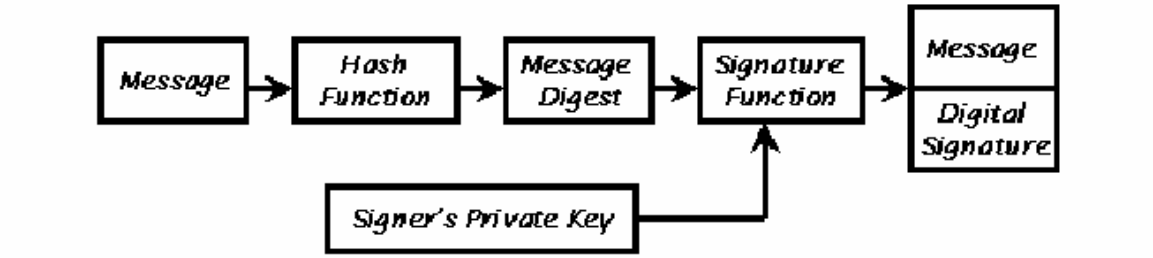

Figure 5 Signature Generation[35]

Signature Verification

The application shall validate the presented certificate and verify the Digital Signature applied to the message to ensure the signer's identity and the message's integrity. Specifically, the signature verification process determines if the signer's certificate is valid, if the signature was created with the private key that corresponds to the signer's public key, and if the message has been altered since the signature was applied. The signature verification sub-process is composed of two activities:

- Certificate Validation
- Digital Signature Verification
    - Certificate Validation

For the presented public key certificate, determine the validity of the public key and the identity of the subject. This is an iterative process of checking the validity period, revocation status, issuer/subject name chaining, and any name, policy or other applicable constraints for each certificate in the certification path. This certificate validation should be performed in accordance with RFC3280.

Digital Signature Verification

The Digital Signature verification process is described and illustrated below. To verify the signer's identity and the integrity of the message, the verification is performed as follows:

- Calculate the message digest;
- Obtain the public key from the subject public key information field of the signer certificate validated in step a above;
- Apply the public key to the Digital Signature to recover the received message digest;
- Compare the two message digests. If the digests are equal;
- The signer's identity is verified as the subject of the public key certificate, i.e. the signature was created with the corresponding private key;
- The integrity of the message is verified.

[35] SAFE Digital Signature Use and Verification Process Guideline

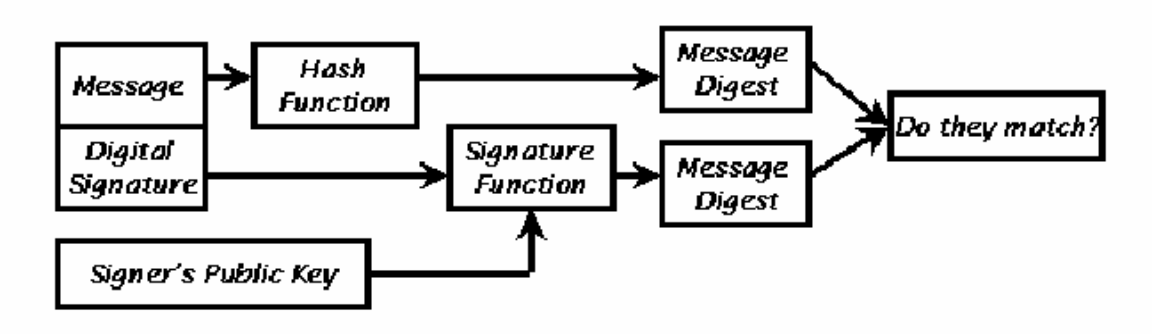

Figure 6 Signature Verification[36]

Credential Lifecycle Management

The life cycle of a digital identity credential can be broken onto the following phases:

- Credential Issuance
- Credential Renewal
- Credential Revocation

Credentials, in SAFE are managed by a Certification Authority (CA). A CA is defined as an Entity trusted by one or more other Entities to create, assign, issue, and vouch for Digital Certificates. The definition also states that a CA issues Digital Certificates (especially x.509 Certificates) and vouches for the binding between the data items in a Certificate. CAs operate a Registration Authority (RA) either internally or via written delegation to a third party. The RA manages the administrative actions required during the life cycle of a certificate. Regardless of whether the RA is internal or delegated, the CA retains the responsibility for the RA's performance.

Certificate Issuance

Certificates can only be issued after an applicant for a digital identity completes the prescribed identity verification process. This process is tightly controlled. Once a subscriber, i.e., an individual who has received a certificate and activated that certificate, they may use it for authentication to systems and also to digitally sign documents if the organizational certificate policy permits these uses. This ability remains with the subscriber for the life of the certificate or until the certificate is revoked.

Certificate Renewal

Within the PKI systems, certificate renewal consists of issuing a new certificate with a new validity period and serial number while retaining all other information in the original certificate including the Public Key. A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the Subscriber name and attributes are unchanged.

Certificate Revocation

Most PKI CPs stipulate that a certificate shall be revoked when the binding between the Subject and the Subject's Public Key defined within a Certificate is no longer considered valid. Examples of circumstances that invalidate the binding include, but are not limited to:

- Identifying information or affiliation components of any names in the certificate become invalid;
- Subject can be shown to have violated the stipulations of its respective Subscriber, Issuer or Member Agreement, or the stipulations of the CP;

[36] Ibid

- Private Key is compromised or is suspected of compromise;
- The relevant Policy Approval Authority (PAA), CA, or organization sponsoring the subscriber suspects or determines that revocation of a certificate is in the best interest of the integrity of the PKI;
- Certification of the Subject is no longer in the interest of the Issuer; or
- Subscriber or other authorized agent (as defined in the Issuer CPS) asks for his/her certificate to be revoked.

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on a certificate revocation list (CRL). Revoked certificates shall be included on all new publications of the certificate status information (whether obtained via CRL or on-line certificate status protocol (OCSP) response) until the certificates expire. Revoked certificates shall appear on at least one CRL.

Interoperability/Extensibility/Scalability

There are numerous architectures for the operation of a PKI infrastructure. These include:

- Single certification authority which provides all the certificates and CRLs for a given community of users. Users in this architecture can only accept certificates form their CA and new CAs cannot be added to the architecture. Obviously, this architecture does not scale well.
- Basic trust lists provide individual users the means to establish a list of CAs they will trust. There are no relationships among the trusted CAs. While it is easy for the user to add new CAs to their list, there are significant potential issues related to potential certificate compromise of a trusted CA certificate and the ability to maintain information about the trusted CAs since the trusted CAs have no direct connection to the user and, in fact, may not even know they are on a trust list.
- Enterprise Architectures in which CAs establish trust relationships with other CAs within the same enterprise. An enterprise might be a single company, a government agency or a community of users. Within the enterprise architecture the following subsets may be found:
    - Hierarchical PKI in which multiple CAs may provide services and they are all related through a single root CA in a superior-subordinate relationship. This architecture is more scalable since the root CA may issue a certificate to a new subordinate CA, or one of the subordinate CAs may issue a certificate to a new CA that then becomes subordinate to that CA. Figure 4 displays this architecture.

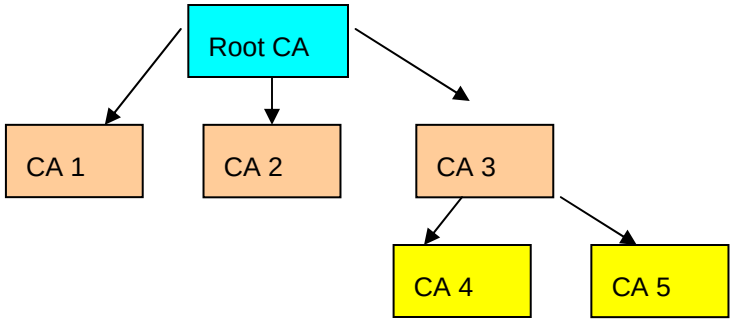

Figure 7 Hierarchical PKI

- Mesh PKIs in which multiple CAs are related in a network of trust on a peer-to-peer basis as shown in Figure 5. In the mesh, each CA exchanges a certificate with other CAs it wishes to trust. New CAs can be easily added. One issue with a mesh architecture is it becomes somewhat more difficult to build certificate paths to validate certificates issued within the network. Also, since the network is a peer-to-peer relationship, one CA cannot impose restrictions on the structure of another CAs certificates and certificate policies may not equate.

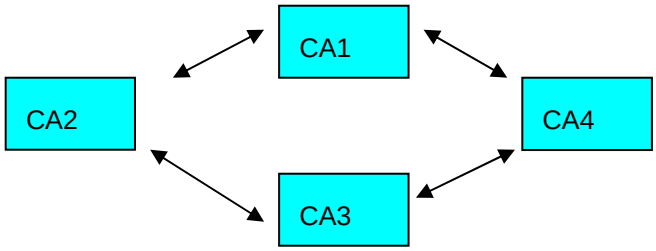

Figure 8 Mesh PKI

- Hybrid Architectures which combine features of the preceding architecture to enhance scalability, technical and operational issues. Hybrid architectures include:
  - Expanded trust lists which may include single CAs, hierarchical PKIs, mesh PKIs or any combination thereof. Although the use of this architecture may reduce the actual number of points of trust, certificate path construction is complicated, management and scalability become more difficult, and the issue of CA certificate compromise remains.
  - Cross certified enterprise PKIs (Figure 6) in which the CAs serving multiple communities or enterprises choose to establish peer-to-peer relationships by reviewing each others' certificate policies and practices to ensure the are equitable and can be trusted to interoperate with each other. This simplifies operations for the user, since, once cross certified, users can trust certificates issued by any of the cross certified PKIs. This mechanism does not scale well beyond a few cross-certified enterprises because of the number of relationships which must be maintained.

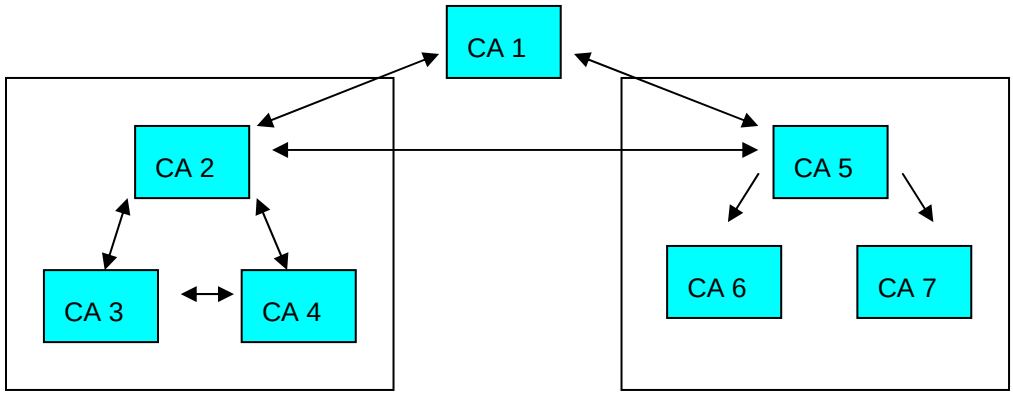

Figure 9 Cross Certified Architecture

  - Bridge Certification Authorities reduce the complexity of cross certification among larger groups of PKIs. Bridge CAs serve as trust arbiters in that they do not issue certificates to end users, but rather issues certificate to root CAs in

hierarchical or mesh PKIs based on policy mapping to ensure the policies of the "bridged" CAs are equivalent and not in conflict. The fact that there is a bridge is transparent to the end users in the cross certified PKIs. The use of bridge CAs simplifies the relationships among the PKIs that are included in the expanded trust network. The bridge established peer-to-peer relationships with the principle CAs in the cross certified PKIs.

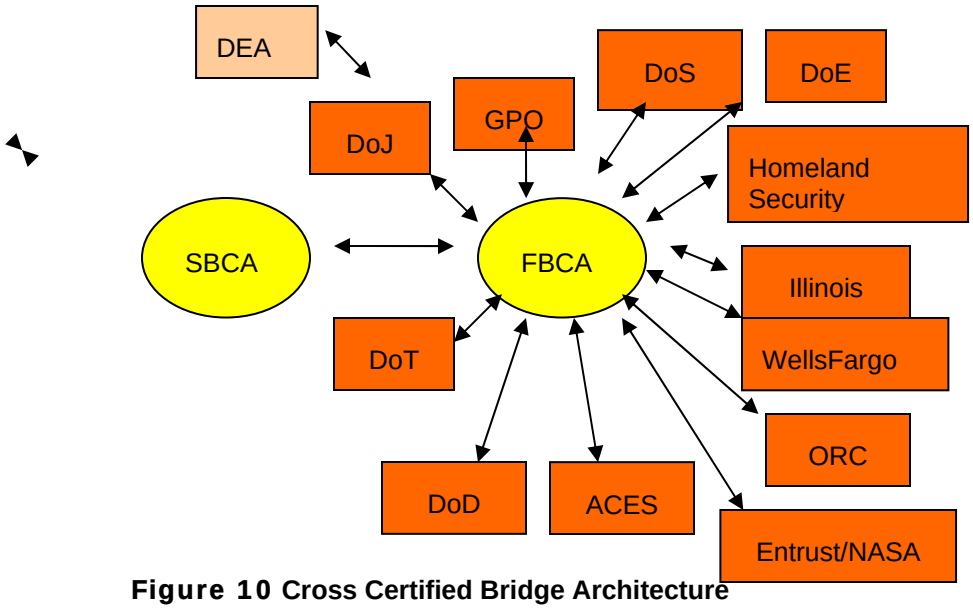

Figure 10 Cross Certified Bridge Architecture

Figure 7 shows this relationship. In this actual example, the SAFE Bridge Certification Authority (SBCA) and the Federal Bridge Certification Authority (FBCA) have cross certified with each other. If the PKIs that are cross certified with the SBCA and FBCA wanted to interoperate without the two bridge CAs, they would have to establish peer to peer relationships with every other PKI in the network--a significantly more difficult set of relationships to maintain. In the bridge architecture, each root CA of the cross certified PKIs cross certifies with a bridge CA. The SBCA and the FBCA then cross certify with each other. This brings all the PKIs that have cross certified with either the SBCA or the FBCA into the network of trust. End users in any of the PKIs can now trust identities and certificates issued from any of the PKIs in the entire network. The bridge architecture facilitates scalability since new CAs or entire PKIs may be added to the network simply by cross certifying with one of the bridge CAs. In a bridge architecture recovery form a compromised CA is also easier since the bridge CA has only to revoke the certificate it issued to the compromised CA and that CA is removed from the network. In a non-bridged architecture, each peer CA with which the compromised CA was cross certified would have to revoke the certificate it had issued to the compromised CA.

While the displayed cross certified architecture does expand the system of trust of each of the cross certified PKIs, the resulting system DOES NOT imply that every user in any of these organizations would be trusted by every other user for every type of transaction. Additional constraints can be placed at the organization and application levels in order to limit trust when it makes sense. The relationships of the PKIs allows a strong authentication of users in other enterprises to be performed; the other three A's (authorization, access control, auditing) remain in the control of the relying party.

Appendix C - About the Biopharmaceutical Industry Digital Identity and Signature Standard

SAFE-BioPharma is a not-for-profit association formed by leading companies within the biopharmaceutical industry to develop and maintain the SAFE standard. The SAFE Standard provides a business, technical and compliance-based framework to assure identities, support user authentication to systems and infrastructures, and also provide a standardized means to apply and manage digital signatures on regulatory and business-to-business documents. Because SAFE is built on a series of contractual agreements among the members, certificate issuers and SAFE itself, it applies on a global basis and the SAFE digital signature strengthens the non-repudiable characteristics of the resulting signature over and above other purely electronic signatures solutions.

The SAFE system of trust operates under the contractual arrangement as depicted in Figure 11 with all participants in the system bound by contract to adhere to and abide by the SAFE Operating Policies, Guidelines and Specifications.

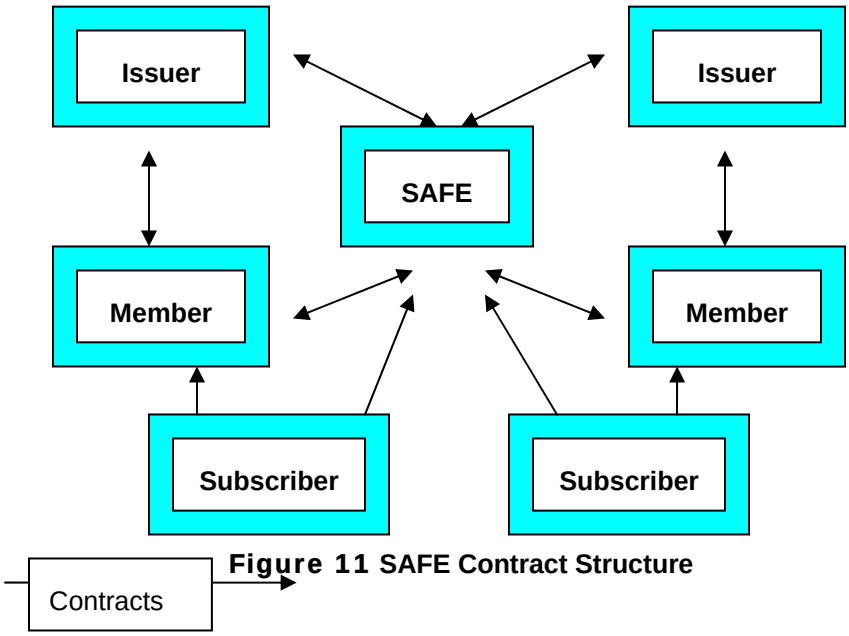

Figure 11 SAFE Contract Structure

This contractual structure eliminates a significant issue in the enforcement of signatures and also in the resolution of any disputes that might arise in business operations. All participants in the SAFE system of trust agree that a signatory will affirm, as part of the signing process, that the signature they are applying shall be considered a SAFE signature under the rules of the system in those instances that apply. If they do not choose to have the signature be covered under the SAFE rule set, they do not perform the attestation.

The SAFE standard complies with the requirements of 21 CFR, Part 11 and facilitates compliance of systems implemented using the SAFE standard with applicable regulatory requirements. Although developed initially for use in the biopharmaceutical drug development space, SAFE provides a baseline to support other healthcare environments in which a strong identity management schema and tight binding of signatures and identities to specific individuals to assure identity is required. The next sections of this paper provide insight into SAFE from the perspective of possible uses and contributions to the broader healthcare delivery arena.

- **Establishing Identity**

SAFE currently conducts its identity authentication (I&A) in manner that complies with the NIST guidance as defined in NIST Special Publication 800-63, Electronic Authentication Guideline and also with the policy of the Federal Bridge Certification Authority (FBCA). SAFE currently operates with Level 3 (Medium) Assurance identities. All I&A activities are performed as a face to face interaction in one of two ways:

- Between the applicant for a certificate and a Trusted Agent (TA), delegated by SAFE to perform I&A; or,
- Between the applicant and a notary public.

Upon completion of the face to face meeting, the TA or the notary forwards completed documentation to the Registration Agent who reviews, approves and directs the certificate issuing authority to issue the certificate to the subscriber.

SAFE also uses antecedent data when applicants are employees of a SAFE member company. In these cases, the TA may rely on identification data that was obtained as part of the on-boarding process for employees. Such information is routinely gathered and maintained as part of the required I-9 process that establishes an individual's right to work. The identity documents used in this process are also routinely used in I&A processes in the federal government under the provisions of the FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors program. In these cases, the TA uses an employee badge as the source of ID and data from the badge is provided to the RA.

The NIST guidance supports remote, or self-registration, I&A. Such a method would undoubtedly be more scalable, especially when dealing with smaller practices and organizations. This would also be significantly more acceptable when individual patients become part of any system. It is crucial that patients have access to their own records. It is also absolutely critical that patient identity be vetted just as that of any other participant. SAFE is currently investigating the capability for self-registration and will most likely have such a capability in effect by the end of 2007. There are, however, potential implications in implementing self-registration with regard to interoperability and cross certification with the Federal Bridge Certification Authority since the FBCA Certificate Policy does not authorize self-registration at this time. Cross certification with the FBCA might require some changes to the Federal Certificate Policy.

It is most likely that any identities used in support of EHI would not need any higher assurance than Level 3 and many could be Level 2 assurance. The primary Level 4 assurance case at this time relates to the use of digital signatures for electronic prescriptions for DEA controlled substances.

SAFE Digital Signatures

As developed and managed by SAFE-BioPharma, SAFE digital signatures meet the specific regulatory requirements of 21 CFR, Part 11 and also meet the requirements of the European Union for digital signatures as a qualified signature. Figure 5 graphically shows the manifestation of the SAFE signature which includes the signer's name, the data and time of signature and a reason for the signing. The presence of the SAFE logo, in this example, indicates that the signature is intended to be a SAFE signature and covered under the SAFE rule set. The assertion that the signature is a SAFE signature is made during the signing ceremony. Signatures can be applied that are not covered by the SAFE rules by not making the assertion.

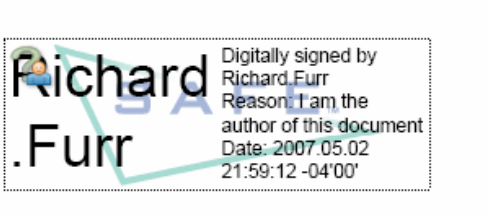

Figure 12 SAFE Digital Signature

SAFE Credential Issuance

Within the SAFE rule set, issuance meets Federal requirements for Level 3 identity authentication for medium assurance certificates and Level 2 requirements for basic assurance certificates. Once a subscriber, i.e., an individual who has received a SAFE certificate, activates the certificate, they may use it for authentication to systems and also to digitally sign documents. This ability remains with the subscriber for the life of the certificate, currently three (3) years, or until the certificate is revoked.