NIST Interagency Report 7601

National Institute of
Standards and Technology
U.S. Department of Commerce

Framework for Emergency Response Officials (ERO)

Authentication and Authorization Infrastructure

Ramaswamy Chandramouli
Teresa Schwarzhoff

NIST Interagency Report 7601

Framework for Emergency Response Official (ERO) Authentication and Authorization Infrastructure

Ramaswamy Chandramouli
Teresa Schwarzhoff

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

August 2010

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Dr. Patrick D. Gallagher, Director

REPORTS ON COMPUTER SYSTEMS TECHNOLOGY

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Interagency Report discusses ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Interagency Report 7601, 18 pages

(August 2010)

Acknowledgements

The authors, Ramaswamy Chandramouli and Teresa Schwarzhoff of the National Institute of Standards and Technology wish to thank their colleagues who reviewed drafts of this document and contributed to its development.

Executive Summary

The purpose of an identity system is to enable individuals to be distinguished from each other in a trustworthy manner. The process of distinguishing one person within a group of people is referred to as *identification*. The process of repetitively affirming the identity of a specific person is termed *authentication*. A capability to reliably authenticate individuals at different times and in different places allows information to be *attributed* to each individual in a correspondingly trustworthy manner. This attribution of additional information (in addition to those required for asserting the identity) forms the basis for authorization of that individual to perform certain tasks. The collection of information used for authentication and subsequently for authorization is called credentials. Jurisdictions, through the issuance of *credentials*, thus can grant and convey recognition of various levels of capability or authority to be exercised by the individual. If there exists an infrastructure for secure exchange of credentials and creation of trust in these credentials, it provides the capability to establish mutual trust and by extension a circle of trust. In this document we describe a framework for establishing such an infrastructure for authentication and authorization of Emergency Response officials (ERO) who respond to various types of man-made and natural disasters. We refer to this infrastructure using the acronym **ERO-AA** that stands for **Emergency Response Official Authentication and Authorization**.

The population of individuals authenticated and authorized under ERO-AA infrastructure include: Federal Emergency Response Officials (FEROs), State/Local/Tribal/Private Sector Emergency Response Officials (SLTP-EROs) and the FEMA Disaster Reserve Workforce (DRW). The system supports the establishment, conveyance and validation of Identity Credentials (ICs), Attribute Credentials (ATs) and Deployment Authorization Credentials (DAC). Apart from enumeration of the types of EROs and their associated authority domains (called major players) and types of credentials, the conceptualization of the framework for ERO-AA infrastructure includes detailed description of various component services under three major service classes: Credentialing Service Class, Identity Verification and Attribute Validation Service Class and Trust Federation Service Class.

The framework is predicated upon the use of trusted tokens capable of supporting biometric as well as secret key based identity authentication. It anticipates the use of various credential mechanisms, specifically including digital certificates, for the trusted conveyance of identification, capability and authority information. The framework is further predicated upon adherence to both technical as well as procedural standards. To the greatest extent possible, existing *de jure* as well as *de facto* standards will be utilized. When absolutely necessary, enhancements to existing standards or the development of new standards will be suggested.

While the framework is specifically targeted at the indicated officials and their corresponding credentials, exploiting a standards based architecture will allow an orderly evolution of capabilities and authorities.

Table of Contents

List of Figures

1. Overview

This document defines the conceptual framework that will provide the blueprint for the design and implementation of a trusted, interoperable Emergency Response Official Authentication and Authorization (ERO-AA) Infrastructure.

The primary purpose of the ERO-AA infrastructure is interoperable secure and reliable authentication and subsequent authorization to needed tasks of first responders, referred to Emergency Response Officials or EROs, at sites that are the scene of a terrorist attack or natural disaster. These are generically referred to as *Emergency Incident sites* in this document. The official responsible for the authentication and authorization functions is referred to as the *Incident Commander*. The organization to which EROs are affiliated is referred to Emergency Management Agency (EMA).

It is anticipated that the following will be major players in the ERO-AA infrastructure:

Federal Agencies (other than FEMA) that maintain a contingent of employees who are deployed for emergency management tasks (e.g., Center for Disease Control, Pentagon)

State/Local/Tribal Emergency Management agencies

Private sector (both for-profit and volunteer) providers of emergency management services

Federal Emergency Management Agency (FEMA) under the federal Department of Homeland Security (DHS)

The framework envisages an infrastructure that performs the function of authentication and authorization of EROs using a combination of credentials in trusted tokens and trusted back-end data repositories. The reason for the choice of trusted tokens, such as contact or contactless smart cards, is that their inherent security characteristics offer highly resilient trusted platforms for information storage and support of standardized interfaces. The trust in the data residing in back-end repositories has to be established by building a federation or a circle of trust among the ERO-AA infrastructure players and the integrity of the data retrieved from those repositories has to be ensured through use of secure communication protocols..

From the prospective of authentication and authorization functions, any player in the ERO-AA infrastructure, irrespective of the location and nature of an emergency incident, will be playing one of the following two major roles:

Credential & Token Issuer - the authoritative source for credentials and credential-bearing tokens, such as smart cards, and hence referred to as Authoritative Source of Credentials (ASC).

The Authenticating entity or the Relying Party (RP) which is usually the Incident Commander and his/her supporting staff at the Emergency incident or preparedness center.

As the nature of interaction among the ERO-AA infrastructure players is mutual aid, an entity that plays the role of ASC in one incident could play the role of RP in another incident depending upon the designated jurisdictional authority for the event. To support the functions needed to be performed by the above two major roles, the service layer of the ERO-AA infrastructure should provide the following three major service classes. They are:

Credentialing Service Class

Credential Verification Service Class

Trust Federation Service Class

Each of the service classes has many component services and are described in greater detail in subsequent sections.

The Credentialing Service class consists of services that provide for the reliable attribution of information to authenticate persons through the use of various credentials. The information attributed to a person encompasses a wide variety of uses. It may consist of a data that provides unambiguous identity through a pseudonym or a data pertaining to a personal trait such as fingerprint biometric. It may convey authority, for example reliably establishing that a specific person is a law-enforcement official or a medical physician; each being a position that imbues that person with well defined rights and privileges such as the right to make arrests or to administer a medical treatment. The information might convey certification, for example reliably establishing that a specific person is licensed to operate heavy (construction) equipment or fly fixed-wing or rotary aircraft. The information might convey personal characteristics of the specific person, for example a record of inoculations or allergies.

The Credential Verification Service class provides services that facilitate a general interaction framework that encompasses (or is an integral part of) a basic identity system. These services facilitate not only reading of identity credentials from tokens but also retrieval from other sources such as back-end repositories for credentials such as qualifications/ skill sets (referred to as *attributes* in this document) and deployment authorizations. It provides for the repetitive authentication of individuals, establishment of trustworthy authority characteristics of those individuals and recording the relevant details of the interaction. This logging of interactions forms a base for developing local reputation for respondents and allows for post-interaction consequences of the interaction to be applied.

The Trust Federation Service class provides services that will enable one ERO-AA infrastructure player (playing the role of Relying Party) to establish trust in the credentials issued by another player (playing the role of Authoritative Source) so as to authenticate an unknown ERO and authorize that person to perform the appropriate task at the incident site dependent on that person's capability, licensing, certification etc. Each ERO-AA infrastructure player joining the trust federation should execute some pre-defined agreements and meet some quality of service metrics. In our context, many of the metrics pertain to the services under Credentialing Service Class.

It is important at this stage to point out some customer facing applications into which some of the key component services in each of the three service classes are packaged. They are:

Credential Enrollment Application

Token Issuing Application

Credential Verification Application

The credential enrollment application is a package of some services from the Credentialing Service Class. These services include vetting of identity-proofing documents, capture of identity credentials (such as fingerprint biometric) and ERO attributes (such as licensing and certification documents issued by proper authorities). The credential enrollment application facilitates transmission of this information to the respective back-end data repositories through protocols and interfaces within a secure messaging system.

The token issuing application makes use of the provisioning service features under the Credentialing Service Class to perform functions necessary for personalization of a token to be issued to an ERO, such as getting the credentials attested by the trusted authority and populating the token with personalized credentials through a secure process.

The credential verification application provides capabilities for retrieval of credentials from the ERO tokens, identification of the token bearer through interaction mechanisms with the token reader (such as entering a PIN or providing fingerprints), and various protocols for validation of credentials through back-end trust broker systems. Depending upon the trust level required for ERO authentication in incident scenarios, this application has to support multiple authentication use cases and correspondingly the subset of capabilities enumerated above may vary as well from one application to another. If the use case calls for only simple visual authentication and credential validation, the credentialing verification application may be a simple laptop application that displays the token holder's photograph, and other identifying and attribute information such as an ERO designator code from a trusted token. In this instance, the use case may be calling for verification of visual identity credentials and verification of attributes (such as qualification/ skill sets) through ERO designators on the token. If the highest level of trust in authentication of an ERO is required, the use case involving strong binding between the bearer and the token and high levels of credibility in an ERO's attributes may be required. In this scenario, the credential verification application has to support features such as biometric authentication and secure federated protocols from retrieving and validating attribute information from remote back-end repositories respectively for meeting these requirements.

1.1 ERO Types

The EROs encompassed within the scope of this framework include the following types:

Federal Emergency Response Officials (FEROs): This includes all employees and contractors employed by a federal agency who perform functions related to: (a) National Response Framework (NRF), (b) National Infrastructure Protection Plan (NIPP), (c) National Continuity Policy Implementation Plan (NCP/IP), and/or (d) National Incident Management System (NIMS).

State/Local/Tribal/Private Sector Emergency Response Officials (SLTP-ERO): This includes emergency response officials from state, local, tribal and private sectors who must access Joint Field offices or other Federal facilities under disaster response situations.

FEMA Disaster Reserve Workforce (DRW): This includes the FEMA's permanent and reserve workforce assigned to perform tasks in any national disaster, whether a natural or terrorism-related.

The framework assumes that each type is based on the issuance of tokens to individuals encompassed by the respective domain. While the capabilities of such tokens may vary, it is assumed that they will evolve in the direction of providing at least trusted Identification, Authentication and (electronic) Signature (IAS) capabilities.

Reference to ERO throughout this document refers to all three types.

1.2 Credential Types

The ERO credentials included in this conceptual framework can be classified into:

Identity Credentials (IC): These credentials define and subsequently help to verify the identity (a person is who he/she claims to be) of an ERO.

Capability or Authority Credentials (CAT): These define the qualifications such as education, training, experience, physical and medical fitness, certification, and licensing of an ERO. Collectively these form the Job or Position description of an ERO.

Deployment Authorization Credentials (DAC): This is the authority to deploy to a disaster site in response to a request for mutual aid assistance. This may be a Mission Assignment issued by a Federal Coordination Officer pursuant to a request for direct assistance from a State.

The framework assumes that each of these credential types can be represented as standardized digital certificates; e.g. certificates digitally signed in a manner consistent with the Public-Key Cryptography Standard #1 (PKCS#1) and represented in a digital format consistent with the X.509 standard.

1.3 Fundamental Characteristics

The development of the conceptual framework outlined in this paper is based on three fundamental observations regarding the overall dynamics of an ERO-AA infrastructure. They are:

The ERO-AA infrastructure will be made up of distributed computing and communication systems.

Existence of specifications, standards, and guidelines for implementation of various component services under each of the three major ERO-AA infrastructure service classes.

The presence of gaps in specifications, standards, and guidelines that need to be addressed through future work.

2. ERO-AA Infrastructure Service Classes & Component Services

As already outlined in the overview section, our framework calls for an ERO-AA infrastructure consisting of three main service classes – Credentialing Service Class, Credential Verification service class and Trust Federation Service class. The justification for a service-centric view of ERO-AA infrastructure (i.e., supported by a service-oriented architecture or SOA) stems from our perspective that the computing and communication elements (e.g., data repositories and transaction/message processing) of this infrastructure will be distributed across several physical and logical domains of authority and hosted on heterogeneous platforms. Each of these service classes contains several component services that collectively define the functional capabilities of the infrastructure. These component services are enumerated and described in this section.

2.1 Components of Credentialing Service Class (CSC)

Recall that the primary goal of ERO-AA infrastructure is reliable authentication and authorization of EROs and the foundation for enabling this function are the credentials and secure conveyance of credential information. The Credentialing Service Class encompasses the following major activities grouped under three services:

- Specification of source documents for identity vetting and verification of their authenticity collectively called Credential Proofing (CSC-A1)
- Credential Gathering and Representation collectively called Credential Enrollment (CSC-A2)
- Establishment of authority associated with each type of credential through credential attestation (e.g., digital certificate) (CSC-A3)
- Secure storage of credentials in data repositories (CSC-A4) and
- Provisioning of authorized credentials into tokens and authentication points (such as physical access control panels and IT system directories) (CSC-A5).

The three services under which the above activities are grouped (along with associated activities) are:

- Credential Proofing Service – Activity CSC-A1
- Credential Enrollment Service – Activities CSC-A2 & CSC-A3
- Credential Lifecycle Management Service – Activities CSC-A4 & CSC-A5

A brief description of Credential Proofing and Credential Enrollment services is given in section 2.1.2 while the Credential Lifecycle Management Service is described in section 2.1.3.

2.1.1 Authority for Issuance for Credentials/Token

The end-result of all three services under the Credentialing Service class is the issuance of credentials to each eligible ERO based on proofing and enrollment activities and issue of a token containing a subset of those credentials to each of the eligible ERO. Naturally the responsibility for performing these services is the organization to which the ERO belongs – Emergency Management Agency (EMA). Since the EMA is

the credential/token issuer, in our ERO-AA infrastructure, the role of EMA is termed Authority Source for Credentials (ASC). The Credential/Token issuing functions are generally managed either directly by the EMA or through a managed service provider hired by that organization. A quick note is in order with respect to activity CSC-A3. Please note that only the establishment of authority associated with each type of credential is included under the Credential Enrollment Service. The actual credential attestation activity comes under Trust Creation Service (refer section 2.3.2) under Trust Federation Service class.

2.1.2 Credential Types and Associations

Recall that Section 1.2 describes three types of ERO credentials: Identity Credentials, Capability or Authority Credentials and Deployment Authorization Credentials. The Identity Credentials and Capability Credentials pertain to a specific ERO while the Deployment Authorization Credentials generally pertains to the EMA organization as a whole. It must be mentioned here that a digital certificate itself (e.g., PIV Authentication Certificate) can be an identity credential (besides an identifying characteristic such as a fingerprint biometric). To obtain this credential, an *a priori* arrangement with a network of trusted third parties is established. Each of these trusted third parties can issue credentials to individuals where the credentials take the form of digital certificates. The issue of "establishing credence or trust" now becomes more of a problem of "conveying credence". That is, when a token that contains digital certificates is presented, the integrity of the certificate can be verified and then the signature of the trusted third party that issued the certificate can be verified. Through this trusted process, the certificate can then be completely validated. Thus, the credence conveyed is that of the trusted third party conveyed to the receiving party of the certificate.

2.1.2 Credential Proofing & Credential Enrollment Service

The formal association of Identity Credentials and Capability Credentials with an individual ERO (enrollment) can only be performed after an examination of evidences through some source documents. Hence two distinct activities – Credential Proofing and Credential Enrollment are needed for issuance of Identity Credentials and Capability Credentials. The Deployment Authorization Credential is either an incident-specific authorization or a pre-negotiated agreement (e.g., Emergency Management Assistance Compact (EMAC) between states) between two Emergency Management Agencies and hence this type of credential is associated with the entire EMA and not with a particular ERO working in that EMA. Going back to Proofing Service (or Proofing activity since this service consists of only one activity by the same name), we find that proofing is nothing but validation of information on which the credential (especially the identity credential) is based. Since this information is contained in source documents (e.g. Birth Certificate or Driver's License), the proofing activity is nothing but verification of the authenticity of these source documents and thus establishing credence in them.

The primary activity in the Credential Enrollment Service is the enrollment activity that consists of extracting or gathering credentials (e.g., capturing biometric information through a scanner) and then in many cases formatting the credentials into some standard representation formats (e.g., CBEFF for biometric credentials -) to facilitate exchange of these credentials across different entities) before storing them in the credential repositories. Often, the EMA that will be issuing the credentials to EROs through tokens will also designate a trusted third party for attesting the credentials (or indirectly an artifact associated with the credentials – such as the digital signature) so that those credentials can be trusted by any other EMA requesting the services of EROs from this EMA.

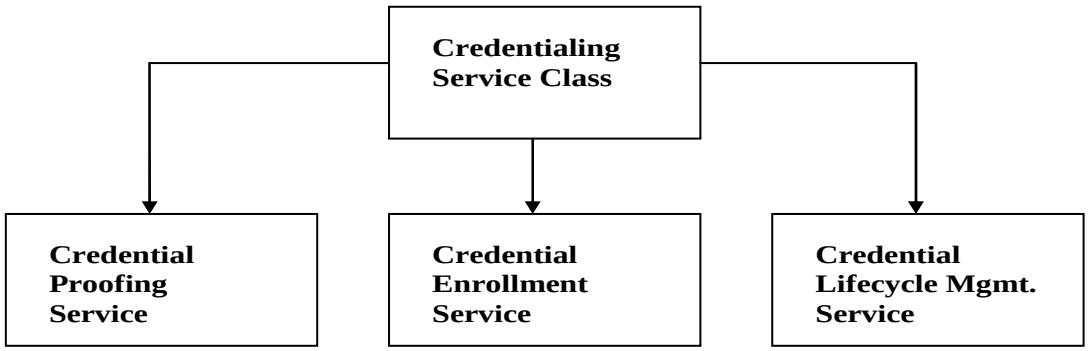

Figure 1: Credentialing Service Class & its Component Services

2.1.3 Credential Lifecycle Management Service

The credential lifecycle management service provides the foundational support for the Credentialing Service class as it deals with activities relating to permanent storage of enrolled credentials and subsequent dissemination of those credentials to all locations wherever authentication based on the credentials is to be performed. The constituent activities under this service are:

Credential Storage: - This activity involves secure, persistent storage of credentials collected during enrollment in a credential repository and subsequently maintains the status of the credential (i.e., suspended, revoked, or expired).

Credential Provisioning – This involves: (a) Personalizing a token with his/her credentials before issuing it to an ERO (using a Token Management Infrastructure) and (b) Disseminating a subset of credentials to authentication points based on the type of authentication applications envisaged for the token (e.g., to a physical access control system/station set up an incident site).

The Credential Storage activity is generally enabled by a class of software systems called an Identity Management System (IDMS).. The Credential Provisioning uses the credentials that have been adjudicated and approved for a particular ERO and stored in the credential repository services to personalize a trusted token using a token management infrastructure. The principal element of a token management infrastructure is a class of software system called Card Management System (CMS).As already mentioned, the credential could consist of a digital certificate issued by a trusted third party or a personal characteristic such as a fingerprint biometric.. For the latter form of credential, the issuer of the token would like to provide a digital signature of the credential and an attestation for itself (the signer) again through a trusted third party. For this it will use the Trust Creation Service (under Trust Federation Service Class) to have its signing key attested.

A compelling, if not primary reason to use secure tokens as central components of identity systems is their standing as trusted platforms suitable for the secure storage of information and the secure processing of sensitive computational procedures. The secure (trusted) storage of information such as credentials is important for both identity credentials (e.g., a biometric template) as well as capability or authority credentials (e.g., ERO designator code).

The connection of a trusted token such as a smart card to a general computer system is accomplished through an *interface device*, typically noted by its acronym of IFD. This is illustrated in a very generic form in Figure 2. The figure also shows the applications that have packaged the token management

infrastructure and some of the services described in our framework to interact with the token. The IFD is accessed by the operating system of the general computer system through a device driver that supports an application programming interface to the IFD. Commands destined for the token itself are sent to the IFD for subsequent transmission on to the token. A significant characteristic of the IFD is the degree to which it enables or supports the establishment of a trusted environment between the token and the computer to which the IFD is connected.

In this regard, IFDs come in many varieties. Indeed, it is a crucial aspect of standards within token systems to allow for interoperability among these varieties. For example, some IFDs are "dumb". They simply convey messages between the computer and the token. Other IFDs are "smart". Rather than simply convey messages, they can be instructed to perform complex protocols, independent from the computer system. Thus, a "smart" variant of IFD might include a PIN keypad such that the computer can instruct the IFD to "get the PIN from the token bearer and send it directly to the token". In this way, token bearer authentication can be done without unduly engaging the potentially untrusted general computer system.

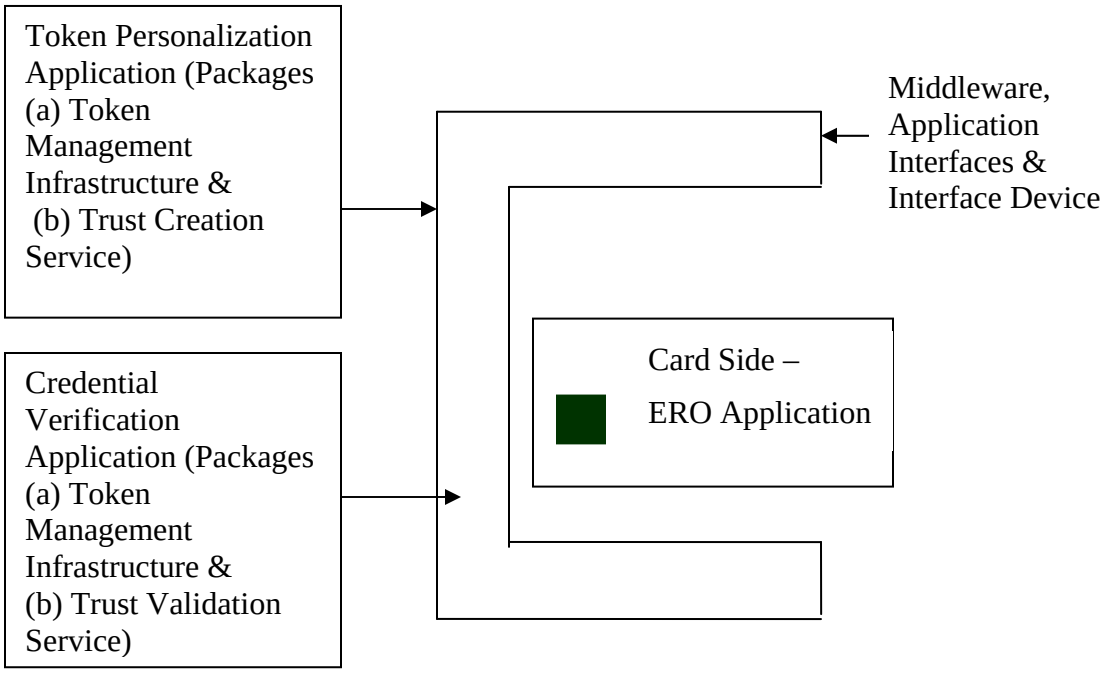

Figure 2: Token Management Infrastructure & Packaging Applications

2.2 Components of the Credential Verification Service Class

Figure 3 depicts the Credential Verification Service Class and its component services:

Identity Verification (IV) Service (Authentication)

Capability/Authority Validation (CAV) Service

Transaction Logging Service (for IV and CAV Transactions)

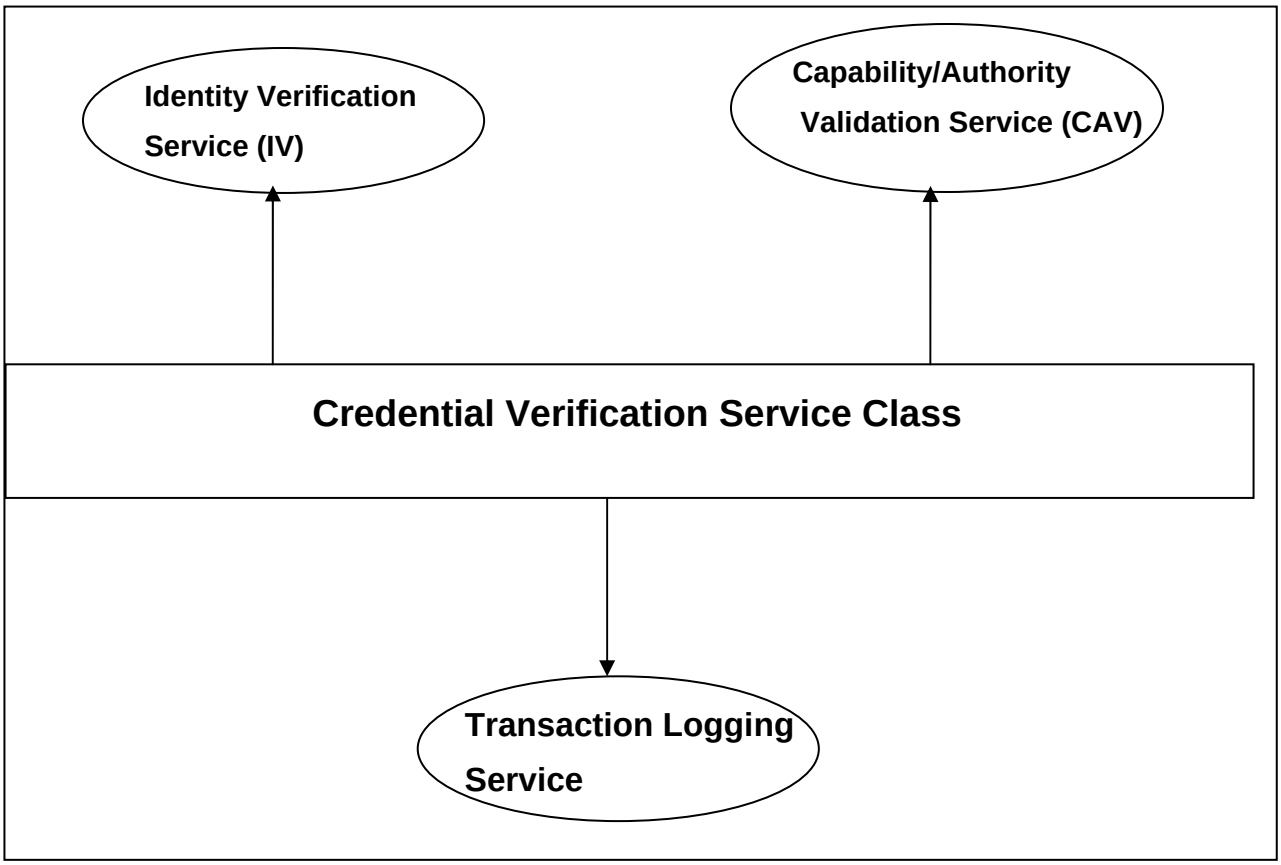

Figure 3: Credential Verification Service Class & its Component Services

The services in this Class are used by the relying party when an ERO presents a token. The first step in the interaction is typically to authenticate the identity of the token bearer. This involves querying the token to retrieve the identity credentials and then validating those credentials to affirm their (information) integrity and the fact that they were issued by known, trusted third parties (to the interaction). Once the identity of an ERO is authenticated, information attributed to that identity must be validated in order to establish capability or authority. for the various tasks that the ERO must perform at an incident site. Last but not the least, the authentication and authorization events must be logged for post-incident reporting and accountability. The post-incident reporting and accountability services are relevant to the resolution and consequences of interactions. In particular, these post-incident services allow for the resolution of discrepancies or disputes regarding the consequences of interactions.

2.3 Components of Trust Federation Service Class

When EROs affiliated with one EMA respond to an incident that is under the jurisdiction of second EMA, the latter has to verify the identity credentials and capability/authority credentials of the responders from the first EMA. This calls for establishing an apriori trust relationship between the two EMAs involved in the interaction. Since this requires lots of pairwise trust agreements, a more scalable infrastructure calls a brokered trust model using a third party. This third party called the Identity Provider should provide services in connection with attestation of credentials when it is first issued by the EMA as well as to validate those credentials when requested by a relying party such as an Incident Commander. These

services by the third party trust broker are classified under the Trust Federation Service Class and consists of the Trust Validation Service and the Trust Creation Service.

2.3.1 Trust Creation Service

When the token-issuing EMA (ASC) provisions certain identifying credential (e.g., fingerprint template) or capabilitycredential to the token, the issuer attaches a digital signature along with the credential object so that the relying party can have proof of origin and non-tampering. In order to have trust in the digital signature, the signing key of the token issuer must be attested by a trusted third party. This attestation is given through a digital certificate that is provided by the trusted third party that contains the signing key of the token issuer. The service that enables this attestation to be obtained is the Trust Creation Service. We have already seen that a digital certificate can also be issued as credential by itself in addition to being an attestation of the signing key of the credential issuer/signor. Both these forms of digital certificates are issued by Certificate Authorities (CAs) and Attribute Authorities (AAs). This service also provides a means to verify the status of those attestations (suspended, expired, revoked etc) through mechanisms such Certificate Revocation List (CRL) and On-line Certificate Status Protocol (OCSP).

2.3.2 Trust Validation Service

The Trust Validation Service enables secure exchange of credentials between the relying party and credential authoritative sources and subsequently receive proof of validations of those credentials. This service is often provided by trust brokers who often interact with multiple proof of trust issuers such as CAs and AAs. Communication between relying parties (such as an Incident Commander) and Authoritative source of Credential (ASC) – the EMA that provides the responding EROs often takes place through these trust brokers. From a standards perspective, this communication has two characteristics:

It has to use any of the standard protocol, such as de-facto federated web-based protocols such as SAML, WS-* or SOAP

The credentialing schema, while it could be customized for the ERO domain, should be based on a standard data modeling scheme such as a Relational Schema, LDAP schema or XML Schema.

With a customized data schema for credential repositories, a Meta Data Service that provides a common view of the syntax and semantics of various ERO capabilities may be required. As previously stated, examples of capabilities include Qualification, Training, Licensing, and Skill Certification documents for various Emergency Response functions as well as apriori deployment agreements among the ERO-AA infrastructure players such as Emergency Management Assistance Compacts (EMACs).

3. Leveraging Standards and Emerging Specifications

A number of technical and procedural standards are central to specifying the components of the framework for ERO-AA infrastructure described in this document. The primary standards are:

- *Federal Information Processing Standard 201 – Personal Identity Verification (FIPS 201) and its companion documents*: These documents specify procedures for identity proofing, the set of credentials and authentication use cases for identity verification, the standardized formats for representation of credentials, procedures for digitally signing credentials and attesting the digital signatures and credentials. and

- *ISO/IEC 24727- Identification Cards – integrated circuit card programming interfaces,*, which provides a set of interfaces for secure, interoperability among diverse applications with normative processes for Identity, Authentication, and Signature (IAS)services. The ISO/IEC 24727 standard is particularly applicable to the framework because it is designed to allow for interoperability of existing stove-pipe approaches and provides for web-based services.

- *National Information Exchange Model (NIEM) standards:* These standards specify the naming conventions and structures for developing a NIEM-compliant XML Schemas. It is necessary that XML schemas developed for ERO job descriptions from various ESF categories should conform to these standards in order to facilitate exchange of emergency management information with other constituencies such as Law Enforcement agencies etc.

Since the publication of FIPS 201 in 2005 and ISO/IEC 24727 in 2009, a majority of Federal employees and contractors have been issued PIV credentials, having gone through an identity proofing process before being issued their credentials. This has resulted in the following developments and emerging specifications which will have an impact on the ERO-AA infrastructure.

- *Personal Identity Verification for Non-Federal Issuers (PIV-NFI) & Revised X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)*: With the increasing use of PIV tokens, there is a great deal of interest from parties external to the government and who want to do business with the federal government to issue identity cards that are technically operable with federal government PIV systems and are issued in a manner that allows federal relying parties to trust the cards. To facilitate this, a set of minimum requirements for non-federally issued identity cards have been provided in the PIV-NFI document that has been issued by the federal CIO council. The associated trust requirements for these identity cards are specified in the FBCA profile document.

- *Federal Identity, Credentialing and Access Management (FICAM) - Open ID and Identity Metasystem Interoperability (IMI) Profiles:* In order to facilitate exchange of business transactions between federal government agencies and its business partners and constituents, the FICAM subcommittee (that has been established by the Federal CIO council) has already developed profiles for industry developed federation protocols as a means of adopting them for meeting the requirements for various levels of authentication for doing business with the federal government.

4. Summary

A conceptual framework for an infrastructure for reliable authentication and authorization of EROs is described in this document. The target communities for the ERO-AA infrastructure are: Federal Emergency Response Officials (FEROs), State/Local/Tribal/Private Sector Emergency Response Officials (SLTP-EROs), private sector providers of emergency management services and the FEMA Disaster Reserve Workforce (DRW). The system supports the establishment, conveyance and validation of Identity Credentials (IC), Capability/Authority Credentials (CAC) and Deployment Authorization Credentials (DAC).

The functional dynamics of the framework is described under 3 broad service classes (Credentialing Service Class, Identity Verification and Capability/Authority Validation Class and Trust Federation Service Class) that provide key services such as enrollment of credentials for the target community of EROs, provisioning of credentials to trusted tokens, and verification of identity and validation of capabilities/authority through secure, interoperable protocols. The credentials include identity, capabilities/authority conveyed through training and certifications etc, and deployment authorizations in the form of pre-defined agreements. The design of services and packaging of services into applications (and their associated architectures) under the ERO-AA infrastructure framework has to be based on adherence to both technical as well as procedural standards. To the greatest extent possible, existing *de jure* as well as *de facto* standards should be utilized. When absolutely necessary, amendments to existing standards or the development of new standards should be considered. The emphasis on standards in the framework for ERO-AA infrastructure is to develop a working architecture for implementing the infrastructure that allows an orderly evolution of capabilities and authorities.