4.0 Security Architecture

The Government Electronic Directory will provide security mechanisms for protecting and safeguarding information that it contains and provides to Government users and applications. The Government Electronic Directory is a fully distributed system. The security framework allows users to access information for which they are authorized through access control mechanisms. Thus enabling secure access to data wherever it may be maintained in the Government Electronic Directory domain. A combination of hardware, software, administrative procedures, and physical placement of components provides the security framework that enables the Government Electronic Directory to comply with the Computer Security Act of 1987.

The 1993 ITU-T X.500 Directory Services standard defines two mechanisms for providing security of the information held in the Government Electronic Directory:

- Authentication Framework -- Verifies the identity of the user or application requesting access to the directory

- Access Control Framework -- Allows the owner of information in the DIB to limit and restrict operations on directory entries.

In the context of Government Electronic Directory, the issue of security is important from a directory knowledge perspective. As stated previously, the data in the DIB will exist in one or more DSAs. When a DUA requests directory information on behalf of an end-user or application, the DSA will fulfill the request using whatever method had been designed and implemented into the DSA topology. The directory data will either be returned through a chaining of requests by interconnected DSAs or by directly reading a DSA from a copy of the appropriate information. In either case, it is possible that various data elements could be accessed by unauthorized individuals or computer applications. To preclude the destruction or misuse of directory information by unauthorized users, certain security mechanisms have been integrated into X.500.

4.1 Authentication Framework

The 1993 ITU-T X.500 Directory Services standard includes the X.509 Authentication Framework, which specifies the information that may be stored in the X.500 Directory, and the procedures that may be used by the Directory and users of the Directory to authenticate each other. The X.509 recommendation defines the authentication framework using certificates and public key information.

Authentication verifies the identity of the individual or application that desires access to the directory. Furthermore, X.500 supports Access Controls that define which individuals may view specific information stored in the DIB. Access controls are based upon the premise that individuals can be uniquely identified using either simple or strong authentication. Access control information establishes who may see what information based upon their identity. Without adequate authentication, access controls are of no value.

Authentication also provides non-repudiation services which protect against denial of involvement in a transaction by providing irrefutable evidence, typically through the use of digital signature technology. In other words, any end-user involved in an electronic transaction using strong authentication cannot deny that he or she was involved in the transaction. It may be the case that someone wants to use the X.500 directory to gain information for a particular Government agency. If the user electronically submits the request, he or she cannot deny that it was he or she who requested the information. The X.500 Directory Model supports two levels of authentication:

- Simple Authentication -- Uses a password and DN pair as a verification of the individual's or application's claimed identity

- Strong authentication -- Uses credentials formed using cryptographic techniques that require the implementation of a support infrastructure to manage the distribution of public keys and certificates.

The authentication scenario in X.509 provides a method by which all DSAs in a distributed directory share a common level of trust; a user is authenticated to a home DSA and any DSAs subsequently accessed will accept the results of the home DSAs authentication results. The 1993 X.500 recommendations provide for an indication of whether a DUA has strongly authenticated itself to a DSA or not.

4.1.1 Simple Authentication

Simple Authentication is based on a combination of the DN and password provided by an entity (application or user) authenticating itself to the DSA. Together the DN and password provide a unique identity to the Government Electronic Directory. The user or application forwards its DN and password through the DUA interface. The password may be transmitted in clear text over the network (simple authentication), or it may be protected using a one-way hash function to encode the password prior to transmission over the network (simple protected authentication). The DSA that authenticates a user or application checks its DIB for an entry which corresponds to the DN sent with the DUA's DAP Bind request. If the DSA locates the corresponding entry, it then uses the Compare operation to see if the password forwarded by the DUA (e.g., user or application) matches the value stored in the `userPassword` attribute for the entry. To decode a protected password transmitted by a DUA the DSA will use the same hash function used to encode the password. When using protected passwords, the object identifier of the hashing function that was used to encode the password will be contained in the DUA's DAP Bind request.

Simple authentication, which transmits passwords in clear text, is the least secure form of authentication defined by the current standards. This level of security is usually sufficient in environments where security is not a major concern.

4.1.2 Strong Authentication

Strong authentication is based on asymmetric public key encryption techniques. Digital signatures are applied to this information passed in the Bind operations that take place between X.500 components.

The X.500 standard does not mandate a particular encryption algorithm. Strong authentication requires the use of an asymmetric Public Key CryptoSystem (PKCS). Each entity (user or application) using the PKCS must have two keys:

- Private Key -- This key is used to generate digital signatures for electronic documents. The Private Key is stored on a token device to ensure that it is in the possession of the signer of the document. All computations will be performed on the token device.

- Public Key -- This key is used by the recipient of a digital signed document to verify the integrity of the signed document and secondly to authenticate the identity of the signer. The public key is stored in the `userCertificate` attribute of the entity's directory entry.

Strong authentication requires the user or application (i.e., sender) to send a strong authentication token during the DAP bind operation. The strong authentication token is a digitally signed sequence of the following:

- User DN
- DSA DN
- Timestamp and random number
- Object identifier of the algorithm used to sign the token.

The DSA deciphers the authentication token using the sender's public key, which is stored in the entry that corresponds to the sender's DN.

The X.500 Directory provides an advantage in the usage of these systems in that user certificates are held within the Directory as user information, and may be freely communicated within the Government Directory System and obtained by users of the system in the same manner as other Directory information. User certificates are formulated using "off-line" methods, and then placed in the X.500 Directory by a Certification Authority.

4.1.3 No Authentication

The use of authentication is not a requirement of the X.500 Directory Services standard. Therefore, a third class of authentication (e.g., none) exists in addition to simple and strong authentication. No authentication will be required to support some external (non-government) entities, such as users browsing a subset of the Government Electronic Directory through the World Wide Web or from public kiosks. It will be up to each agency to determine who is permitted to view its subtree (or portion of its subtree) and under what circumstances (e.g., having provided simple, strong or no authentication credentials).

4.2 Certificates

Public keys are stored in the Government Electronic Directory in the form of a `userCertificate` contained in the Directory entry of the entity. Certificates are constructed by "signing" a set of information that includes the DN and Public Key of the entity as well as other relevant data. Certificates are valid for a predefined time period, after which they expire and must be removed from use and replaced with new certificates. The administrative process required to generate and distribute key pairs is outside the scope of the standard; however, the X.509 standard does establish some general guidelines and requirements for the secure management and generation of key pairs. The X.509 standard states that key pairs may be produced as follows:

- A user may generate his/her own key pair, so the secret key is never released to foreign entities.

- Keys are generated by a secure third party, and must be transferred to the user in a secure manner. This secure third party is referred to as a Certification Authority (CA).

4.2.1 Certification Authorities

The Government Electronic Directory supports a certification hierarchy responsible for key management, e.g., generating Public-Private Key Pairs, generating

and maintaining X.509 userCertificates and certificateRevocationLists. A CA is an entity or organization trusted by one or more users to create user keys and to generate and assign certificates.

An X.509 userCertificate binds the user's DN to the public key information. CAs digitally sign each userCertificate before sending it to the DSA for insertion into the appropriate directory entry. The integrity of the userCertificate and the information contained within it are maintained through the use of the CAs digital signature, thus ensuring that no person or process can tampered with the userCertificate. DSAs and DUAs participating in the Government Electronic Directory support insertion and maintenance of userCertificate information in the directory by sanctioned CAs. The express purpose of a userCertificate is to make publicly available the Public Key of the entity and other related information, thus enabling any user to confirm the validity of a received digital signature.

A standard X.509 userCertificate contains a signed sequence of the following attributes (although others may also be defined):

- version -- Version number of the certificate: version 1 (1988) or version 2 (1993)
- serialNumber -- Sequential integer value that provides a unique serial number within the certification hierarchy belonging to the CA.
- signature -- Algorithm identifier for the digital signature used to sign the certificate
- issuer -- DN of the CA
- validity -- Validity period of the certificate specified in UTC format as valid not before and not after
- subject -- DN of user
- subjectPublicKeyinfo -- Algorithm identifier for the Public Key and the Public Key
- issuerUniqueIdentifier -- 1993, version 2
- subjectUniqueidentifier -- 1993, version 2.

4.2.2 Certification Paths

Numerous CAs will be responsible for managing keys within the Government Electronic Directory. These CAs will form a certification hierarchy in which a single root CA will certify subordinate CAs representing each organizational subtree. These subordinate CAs will certify CAs and entities within the organizational subtree. Each CA will maintain an entry in the Government Electronic Directory that will contain a `userCertificate`. An example certification hierarchy is depicted in Exhibit 4-1.

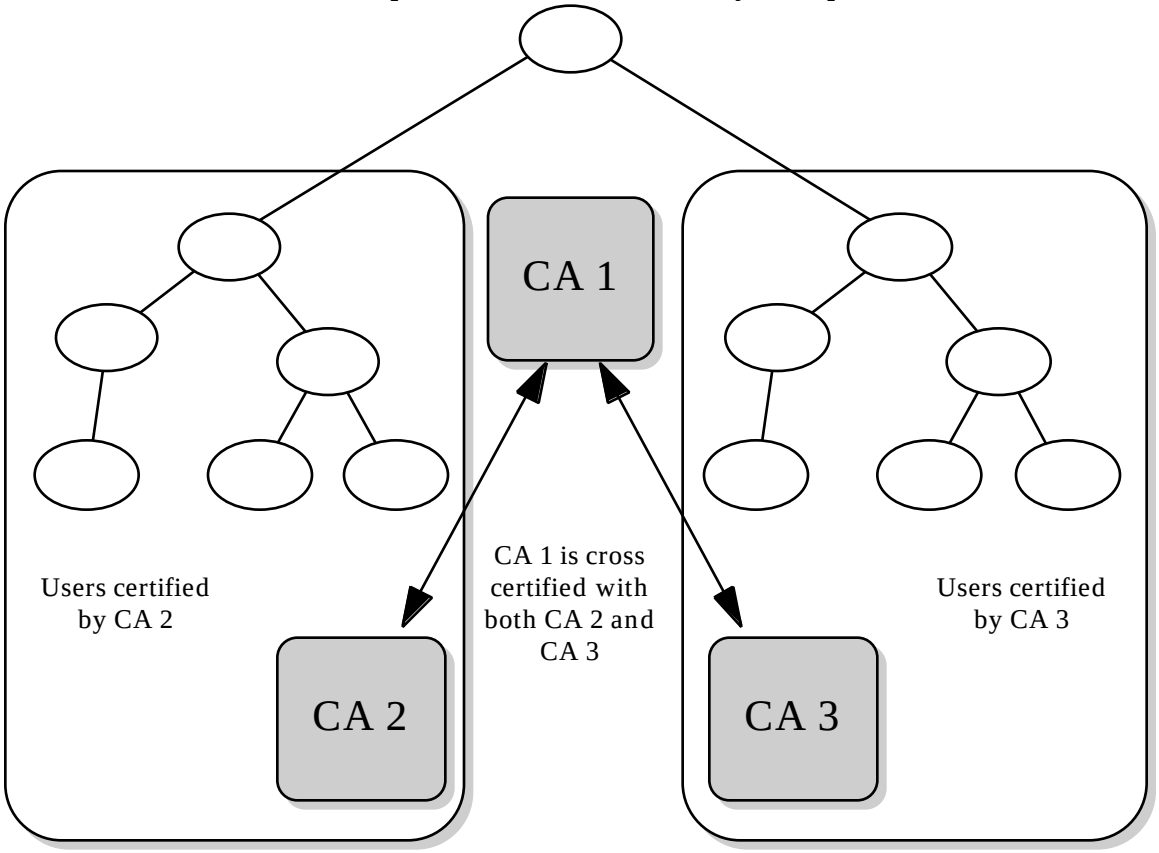

Exhibit 4-1
Certification Authority Hierarchy

When a DSA that uses the services of its own CA needs to chain a query to a DSA which uses the services of a different CA operating within a different certification hierarchy, then the two CAs exchange their `userCertificates` through a bilateral agreement to ensure data integrity between the two DSAs. This exchange of `userCertificates` between the CAs is called a cross certificate pair. Cross certificate

pairs may be considered lists of "trusted DSAs". The chain of certificates between multiple CAs is called a certification path. The certification path can be carried on the DAP or DSP request or result. A certification path, therefore, is used to ensure end-to-end integrity of DUA-to-DSA and DSA-to-DSA communications across the entire Government Electronic Directory. Exhibit 4-2 illustrates a certification path and cross certificate pairs.

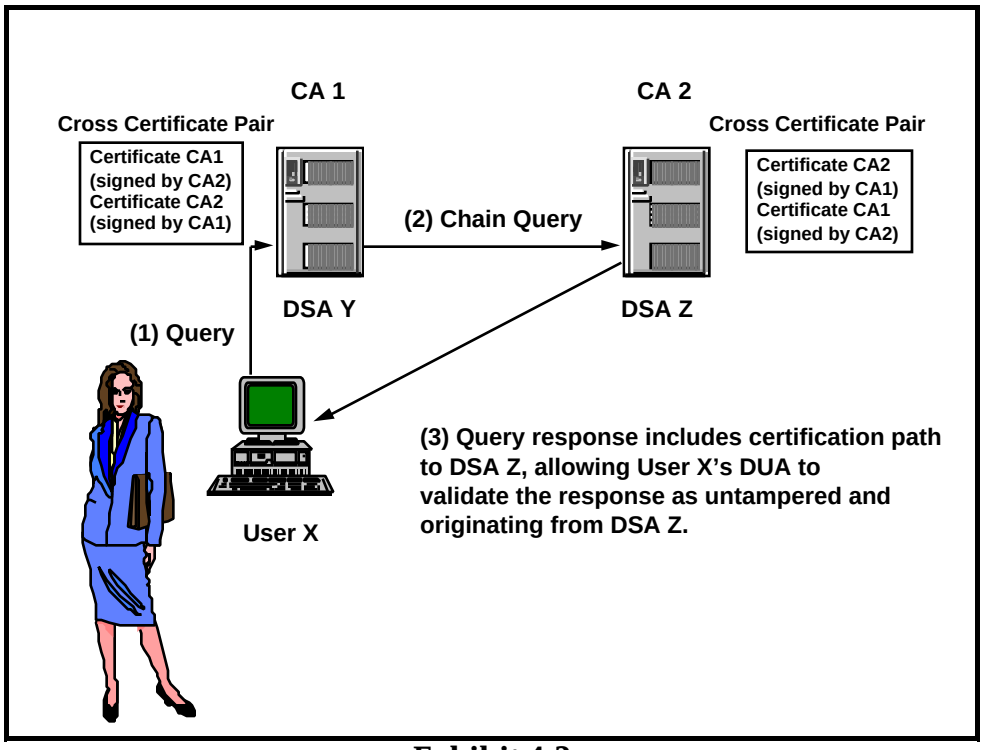

Exhibit 4-2
Cross Certificate Pairs

4.3 Digital Signatures and Data Encryption

Because the Government Electronic Directory furnishes a distributed repository accessible to multiple entities in the network, it will use the X.509 framework to provide data encryption and digital signature capabilities. The Government Directory will also use digital signature capabilities to provide secure, authenticated access to information contained in the directory. The Government directory will use the Digital Signature Standard (DSS) and the Digital Encryption Standard (DES) as specified in FIPS 140-1 and 171. For example, a sender who wishes to send information to a recipient in a

secure manner (i.e., data encryption) obtains the recipient's public key from the Government Electronic Directory and uses it to encrypt the information. The encrypted information is then sent to the intended recipient, who will decrypt it using their personal private key. Exhibit 4-3 illustrates the use of the Government Electronic Directory to perform data encryption using X.509.

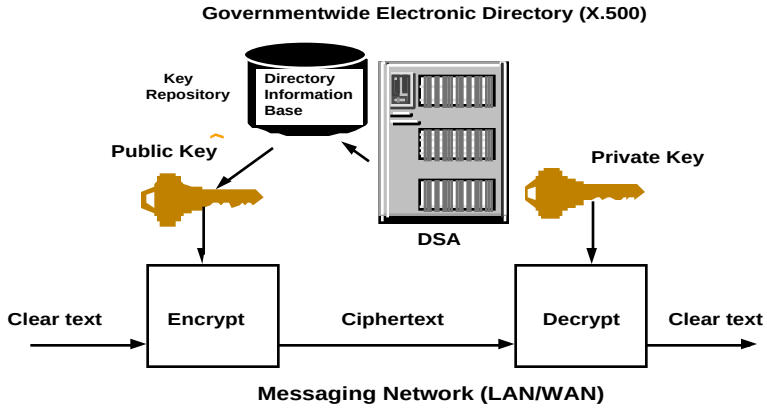

Exhibit 4-3
Data Encryption using X.509

Digital signatures can provide a reliable mechanism for ensuring data integrity. A digital signature is an electronic symbol which can be used to validate the identity of the signer and the integrity of the critical information received from the signer. Legally binding attributes require that digital signatures are:

- Unique to the signer -- The digital signature is generated using an algorithm that takes as inputs the user's Private Key, the electronic document to be signed, and some random value and produces as output a digital signature value that is unique and cannot be replicated.

- Under the signer's sole control -- The user must have in their possession a token (e.g., Smart Card, Fortezza Card) that enables them to generate the digital signature on the token. Furthermore, the token should require the entry of Personal IdentificationNumber to ensure that only the specified user may use it.

- Capable of being verified -- The digital signature may be verified by the recipient by taking the signer's Public Key and the document and performing a digital signature verification operation. The result will confirm the identity of the signer and the integrity of the signed data.

- Linked to the data being signed -- The electronic document is an input to the algorithm employed for signature generation and verification process. Therefore, any changes in the electronic document prior to the verification process would cause a "fail" result to be returned during verification.

The digital signature generation process employs a cryptographic module for managing the digital signature generation. This discussion will focus on the Federal Government mandated Digital Signature Algorithm. The electronic document is first hashed using the Secure Hash Algorithm. The resulting value (message digest) is then passed to the user's token device for generation of the digital signature. The user's Private Key is stored on the token and never leaves it. The signature generation process occurs on the token and the resulting digital signature is returned to the calling application. The electronic document and the digital signature are then transmitted together to the recipient. The process for generating digital signatures using the Digital Signature Algorithm is presented in Exhibit 4-4.

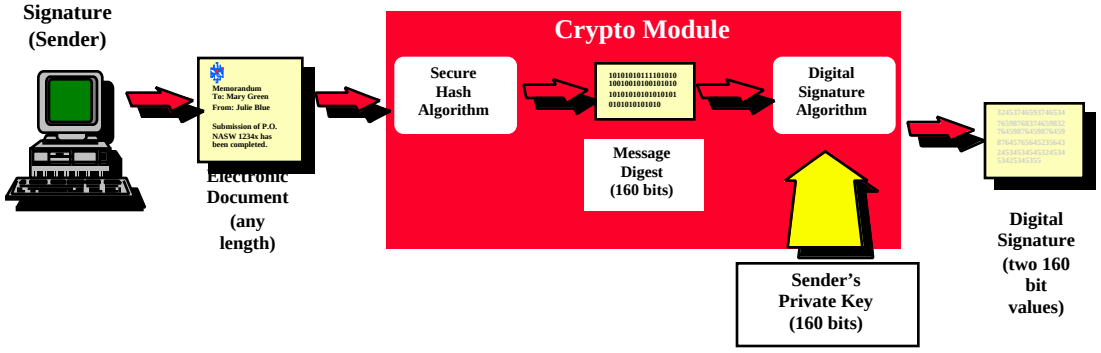

Exhibit 4-4
Digital Signature Generation using X.509

When a user or application receives information that has been digitally signed, it must retrieve the sender's public key from the Government Electronic Directory to

decrypt the signature and ensure data integrity. Exhibit 4-5 depicts the process for verifying a digital signature.

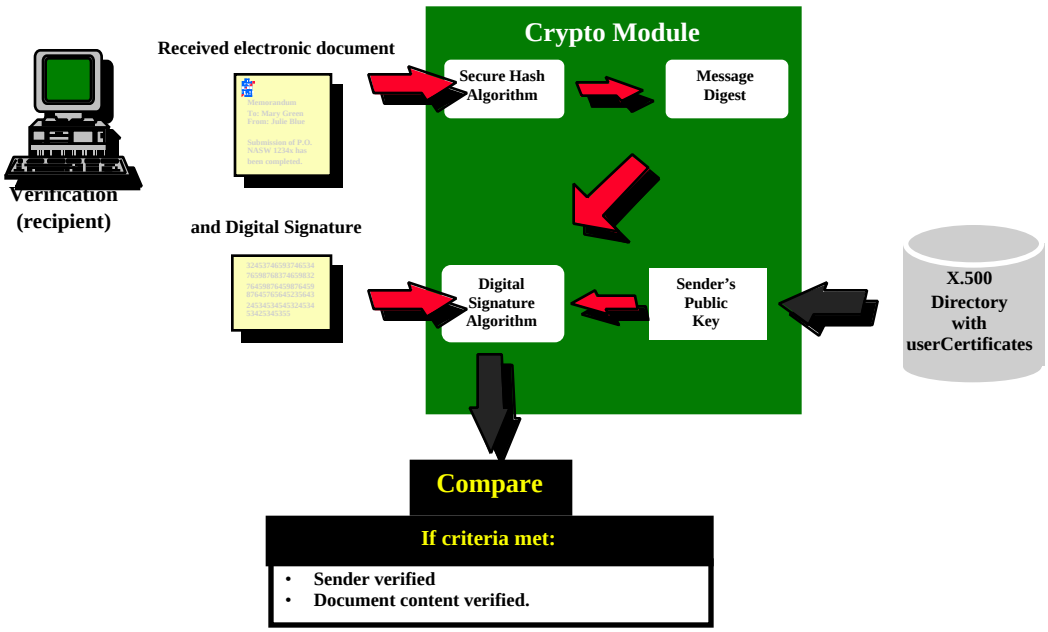

Exhibit 4-5
Digital Signature Verification using X.509

The Government Electronic Directory supports both simple and strong authentication to all directory components on every Directory access, as deemed appropriate by the agency managing each portion of the DIT (i.e., each agency subtree). In addition, the Government Electronic Directory provides the capability to use digital signatures for signing directory operations. Digitally signed operations verify the integrity of the requests and responses contained in both DAP and DSP transmissions from DUAs and DSAs. In this manner, the Government Electronic Directory provides confidentiality services through the use data encryption to protect Directory queries, responses, and information transfers, as necessary. This service also unambiguously verifies that the information marked as originating from a given source (e.g., a DSA) within the Government Electronic Directory domain, did in fact originate there.

4.4 Access Controls

Access control information is used in conjunction with authentication information to allow access to the information stored in the DIB. There are two levels of access control information described in the X.500 (1993) series of recommendations:

- Basic Access control
- Simplified Access Control.

4.4.1 Basic Access Control

The Basic Access Control scheme enables Government Electronic Directory administrators to define access control policies in the form of access control lists. The access control list defines the information being protected (called protected items) along with whom the protected items are protected against (called user classes). In addition, the access control list specifies what actions are allowed against the protected items in the form of explicit permissions. For example, a Government Electronic Directory user may be identified as a member of a particular user class that has Read access to a particular entry or attribute defined as a protected item. The 1993 ITU-T X.500 incorporates an algorithm called the Access Control Decision Function (ACDF) to determine which access control list function applies to a given user/operation request combination based on the level of authentication provided. For instance, the ACDF may determine that a user has read-only access to a particular attribute if the user logs in to the Government Electronic Directory with simple authentication, while granting Modify access to the same attribute when the user logs-in using strong authentication. Thus, the DUA provides the capability to support selective control of access to Government Electronic Directory information by first authenticating the user to the DSA, then providing access rights based on the level of authentication provided.

Basic access control assumes that the identity of the requester of information is well known via strong or simple authentication. The ACDF model defines one or more points at which access decisions take place for every directory operation. These decisions involve:

- Protected items or directory information
- User classes to which the identified requester belongs
- Permission categories available for performing Directory operations
- Scope of application and syntax of access control information items.

The basic access control model allows users permissions to be uniquely defined for each of the following protected items based on the user class of the requester:

- `entry` --
- `allUserAttributeTypes` --
- `attributeType` --
- `allAttributeValues` --
- `allUserAttributeTypesAndValues` --
- `attributeValue` --
- `selfValue` -- The requested operation requested may only be performed when the DN of the originator of the request is the same as the DN or unique member value within the specified attribute. For example, an originator may be able to modify the role occupant of a role if he/she occupies that role.

Basic Access Control defines user classes to which permissions to process information apply including:

- `allUsers` -- Every directory user (with optional requirements for authentication level).

- `thisEntry` -- the user with the same distinguished name as this entry.

- `name` -- the user with the distinguished name specified in the query (with optional unique identifier).

- `userGroup` -- the set of users who are members of the groupofUniqueNames entry, identified by the specified distinguished name. Members of a group of unique names are treated as individual object names, and not as the names of other groups of unique names.

- `subtree` -- the set of users whose distinguished names fall within the definition of the subtree.

The permission categories for operations on directory entries that may be granted to users based on the results of their authentication to the DSA:

- Read -- Display information for a specifically named entry

- Browse -- Permits entries to be accessed using Directory operations which do not explicitly provide the name of the entry (e.g., Search and List)

- Add -- Creation of an entry in the DIT subject to controls on all attributes and attribute values to be placed in the new entry at time of creation

- Remove -- Removes entry from the DIT regardless of controls on attributes or attribute values within the entry

- Modify -- Permits the information contained within an entry to be modified

- Rename -- Granting is necessary for an entry to be renamed with a new RDN, taking into account the consequential changes to the DNs of subordinate entries

- Disclose On Error -- Permits the name of an entry to be disclosed in an error (or empty) result.

- Export -- Entry and its subordinates may be exported, e.g., removed from the current location and placed in a new location subject to the granting of suitable permissions at the destination. If the last RDN is changed, the Rename is also required at the current location.

- Import -- Entry and its subordinates may be imported, e.g., removed from the some other location and placed at the location to which permission applies, subject to the granting of suitable permissions at the source location.

- ReturnDN -- Entry DN value may be disclosed in the result of an operation.

The permission categories for directory attribute and attribute value access are;

- Compare -- Permits attributes and values to be used in a compare operation

- Read -- Permits attributes and values to be returned as entry information in a read or search access operations

- Filter Match -- Permits evaluation of a filter within a search criterion

- Add -- If granted for an attribute, permits adding an attribute (if all specified attribute values can also be added). If granted for an attribute value, it permits adding a value to an existing attribute.

- Remove -- If granted for an attribute, permits removing an attribute complete with all of its values. If granted for an attribute value, it permits the attribute value to be removed from an existing attribute.

- Disclose On Error -- If granted for an attribute, permits the presence of the attribute to be disclosed by an attribute or security error. If granted for an

attribute value, it permits the presence of the attribute value to be disclosed by an attribute or security error.

4.4.2 Simplified Access Control

The Simplified Access Control scheme greatly reduces the computational overhead associated with evaluating a user's access rights. However, Simplified Access Controls do not restrict access to specific attributes and values on a per-entry basis, but restrict access to these attributes and values at the subtree level.

Simplified Access Control provides a subset of the functionality defined for basic access control. It allows access control only for an entire subtree. Entry access control information is not permitted.

4.4.3 Government Directory Schema Security Guidance

It is recommended that each agency participating in the Government X.500 Directory plan to utilize a Basic Access Control scheme that bases access to Government Directory information on the identity of each individual who needs access. Basic access control assumes that the identity of the requester of information is well known via strong or simple authentication. The identity of the requester of information should be based upon membership in a group as defined by the user class **userGroup**, so as to simplify maintenance of permissions for all users. The Government Directory Schema matrix, shown in Appendix D, identifies permission categories for each attribute based upon a possible scenario of group identities. These group identities, while not mandatory, are defined below in order to provide guidance on what access control groups might look like in a typical Government agency.

Self - The requested operation requested may only be performed when the DN of the originator of the request is the same as the DN or unique member value within the specified attribute, or entry. For example, an originator of a directory query may be able to modify the role occupant of a role if he/she occupies that role, or modify their telephone number if they own the telephone number listed All users may be listed as part of this group, with the following operations permitted on their entire

individual entry only: Read, Browse, Return DN. They might be allowed access to individual attribute values (allUserAttributeTypesAndValues) for the following operations; Compare, Read, Filter Match, Disclose.

DSA Manager (DSA Mgr) - Members of this group would be granted full operational access to entries extending to the attribute and attribute value level. In addition to the user operations, such as Read and Browse, they would be allowed to Add, Remove, Modify, Rename entries and perform other DIB maintenance tasks. Agency policy should dictate, in the case of multiple DSA managers, which portion of the DIT may be maintained by each DSA manager, and the information groups restricted accordingly.

Organization User Member (OU Mbr) - Should be further defined by agency policy that dictates what information is generally available inside an organization, versus information that may be viewed by Government Users outside of the organization, or viewed by public citizens. For example, within an organization, all attributes of entries may be viewed (using read, browse, search operations), but certain attributes will be restricted from view by non-organizational, and public citizen directory users. Telephone number, for example, may be available for viewing within the organization for each individual, but not viewed by citizens.

Government User (Gov't User) - In general, users needing access to an organization's data that are not part of the organization would be assigned to this group. This group would restrict information viewed to the non-sensitive level. For example, e-mail addresses may be available to all government employees, but not telephone numbers, or mail addresses.

Authenticated Anonymous (Auth Anon) - This group would be used for individuals that needed access to directory information for a predetermined amount of time, such as in the case of procurement information. Users may be given a password for authentication that will automatically expire when a certain date passes.

Anonymous - (Anon) - This group would be used for general access to the directory for users that use no authentication method. It is envisioned that this access would be

perhaps the most restrictive since public citizens and other unknown entities would be able to view the information.

4.4.4 Access Control Domains

The 1993 ITU-T X.500 standard also provides an administrative model for implementing access controls that secure the information in the DIT. Each subtree of the global X.500 DIT may be partitioned into one or more nonoverlapping access control domains, called Access Control Specific Administrative (ACSA) Areas. For example, the Government Electronic Directory, which is rooted at the subtree beginning at o=U.S. Government corresponds to an ACSA within the global X.500 DIT.

In addition, each subtree within the Government Electronic Directory (e.g., under o=U.S. Government) that corresponds to an agency's portion of the DIT may be delegated its own full or partial security administration. Each access control sub-domain within the ACSA is called an Access Control Inner Administrative (ACIA) Area. ACIAs can be nested, so that an ACIA may further delegate security administration to one or more ACIAs within it. Again, each ACIA is autonomous so that each unit of an organization (i.e., subtree) can be responsible for its own security policies. Exhibit 4-6 provides an illustration of a DIT subtree (ACSA of o=U.S. Government) that contains a single ACIA which is further divided into three separate ACIAs.

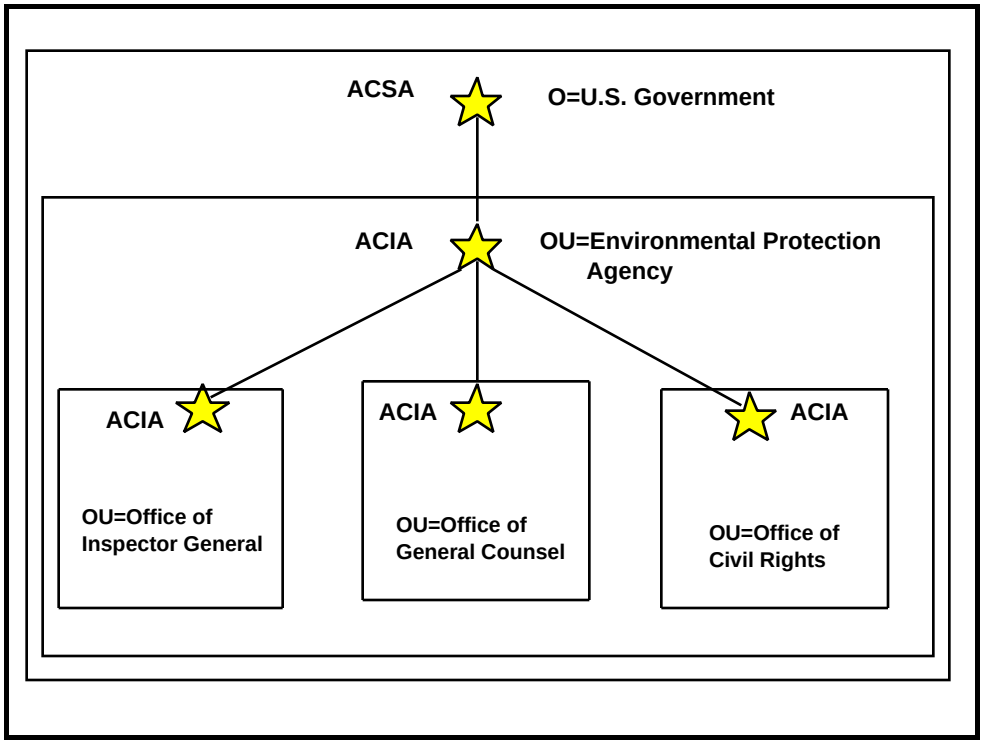

Exhibit 4-6
Access Control Administrative Areas

Where required by a particular ACIA (e.g., an entire agency or a department within an agency), the Government Electronic Directory provides access control mechanisms to the attribute level through Basic Access Control. However, such a requirement is left to each ACIA to implement. In many cases, an agency or department within an agency may determine that Simplified Access Control is sufficient.

4.5 Security Policy

The Government Electronic Directory will institute a security policy that ensures the utmost information integrity. This policy consists of the following three features:

- Security Administration
- Security Accounting
- Physical Security.

4.5.1 Security Administration Features

The security administration features of the Government Electronic Directory include the following:

- Government Electronic Directory systems administrators will use simple protected or strong authentication procedures to obtain administrative access to the Directory. The use of simple or strong authentication will be determined by each agency. Strong authentication, however, is recommended for systems administrators who will be modifying directory entries.

- Each DUA will preclude unauthorized access to its configuration data.

- Security documentation will be required for review and approval of each DSA in the Government Electronic Directory.

- The DSA / DIB memory will be safeguarded for the highest sensitivity of data ever recorded, unless sanitized or destroyed.

- The DSA will provide safeguards against accidental, unauthorized, or malicious actions that result in the alteration of security protection mechanisms or access levels.

- The DSA will provide data integrity services and safeguards against accidental, unauthorized, or malicious actions that result in the alteration of the Directory information.

- No single hardware, software, or human error malfunction will allow security checks to be bypassed.

4.5.2 Security Accounting Features

The Government Electronic Directory will provide accounting mechanisms for logging and tracking use of the Directory. To ensure the highest level of security required by each agency, the Government Electronic Directory will include the following security accounting features:

- The Government Electronic Directory will provide accountability and an audit trail for all queries and will support an analysis of both security monitoring and security-related events (e.g., successful and unsuccessful log-on attempts; violations of security procedures and policies).

- An audit trail of information to support performance monitoring will be provided by the Government Electronic Directory.

- An audit trail of the information to support fault isolation will be provided by the Government Electronic Directory.

- The Government Electronic Directory will generate and maintain audits of all security violations for 30 days.

- The DUA will provide the capability to generate audit trail logs of DUA activities.

- The DUA will ensure against disabling or bypassing of audit capabilities within the software.

4.5.3 Physical Security Features

The Government Electronic Directory will employ safeguards to ensure the physical integrity of the components that make up the Directory (e.g., DUAs, DSAs). To provide this level of physical integrity, the Government Electronic Directory will be protected against physical threats (e.g., intruders, fire, and flood) and electronic and technical failures.

4.5.4 Firewall DSAs

Certain Government organizations (e.g., DoD) may establish DSA firewalls to ensure that only authorized users gain access to selected parts of the DIT. It is anticipated that these DSAs will be implemented for access by the general public and by agencies with requirements to communicate information to / from entities outside of the Government Directory domain and their own agency domain. This topology is shown in Exhibit 4-7.

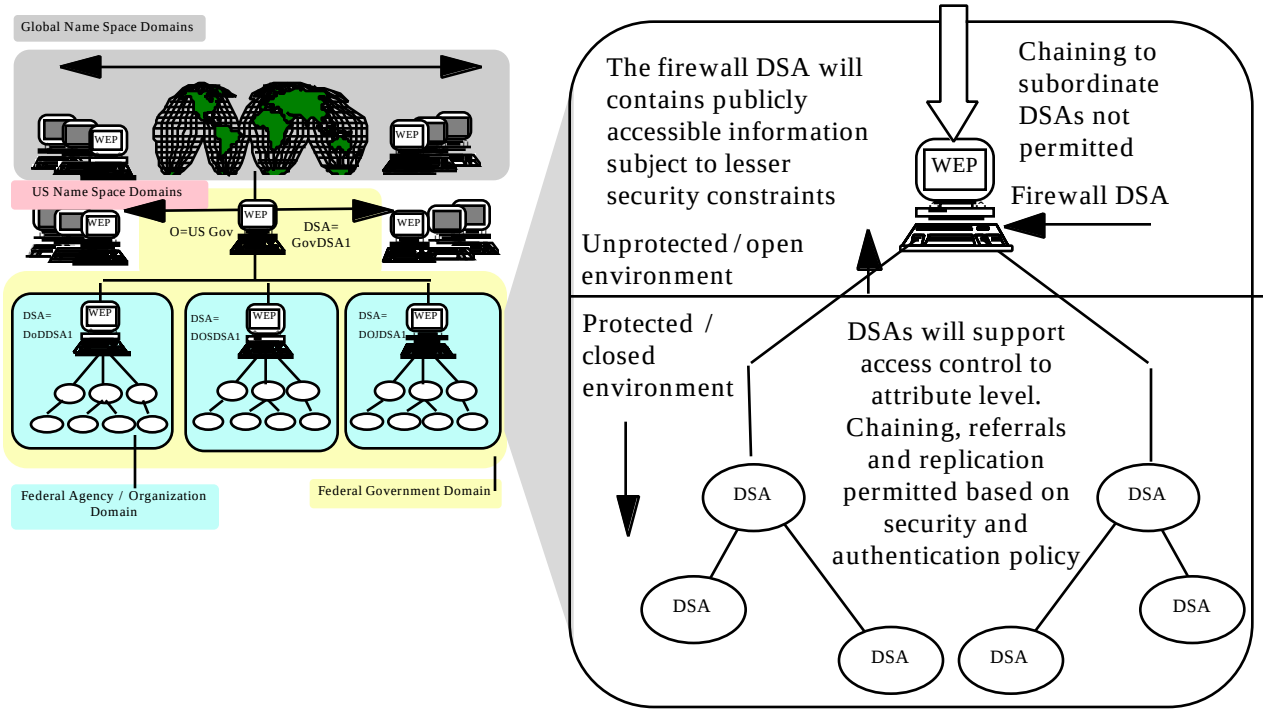

Exhibit 4-7
Firewall DSAs