1.6.7 Managed E-Authentication Service (MEAS) [C.2.10.6]

The managed e-authentication service (MEAS) is a tested and proven, fully managed, customizable security solution that allows the Agency to safely conduct electronic transactions by users who are authenticated to an Agency information technology (IT) system. Developing, supporting, and deploying information security services to meet the demanding requirements of the U.S. Government and corporate customers have refined our MEAS.

1.6.7.1 Technical Approach to Security Services Delivery [L.34.1.6.1]

1.6.7.1.a Approach to Service Delivery [L.34.1.6.1.a]

(a) Analyze the service requirements specified in this solicitation and describe the approaches to service delivery for each service. [L.34.1.6.1.a]

The Agency's needs for E-Authentication services will be fully met by AT&T through our production security systems supplied by the world's leading experts of secure token, PKI, and biometric authentication technology. Our security solution serves users worldwide in the Government, financial services, healthcare, telecommunications, and other industries to protect their networks and data assets from unauthorized access to their internal and external users.

AT&T offers two (2) technical solutions that are flexible and scalable enough to meet MEAS requirements. The first service, a managed token offering, is an access security system that provides exceptional protection to an Agency's information systems through a strong two-factor authentication solutions based on [redacted] technology.

Called strong two-factor authentication, Token Authentication service requires a user to provide: 1) a secret password that they have

memorized, and 2) a secret code randomly generated by a physical device (token authenticator) in the user's possession. **Figure 1.6.7.1-1** illustrates delivery of our managed token authentication service. Delivery of this service consists of the following components:

- **Shared or Dedicated Token Authentication Server**. The server controls the user-authentication aspect of the service, using a central database for administration of user accounts and security policies.
- **Token Authentication Agents**. Agents provide the interface for users desiring access to protected resources to enter passwords and token codes. Agents are device-specific software built into protected network equipment on the customer's premises. The products of more than 140 leading vendors of firewalls, remote access servers, VPNs and Web applications support two-factor authentication right out of the box, so it is likely the Agents are already in place.
- **Token Authenticator**. An authenticator is a small, user-carried key fob device. Each authenticator contains a unique [redacted] that is combined with a powerful algorithm to generate a new code every [redacted] Because the number is unpredictable and dynamic, it would be extremely difficult for a hacker to guess the correct number at any given time. Patented technology synchronizes each authenticator with the Token Authentication Server, providing a high level of security.
- **Token Authentication Customer Care Center**. The 24 x 7 Customer Care Center provides customer support and administers the service, including:
  - Distributes and replaces token authenticators to users
  - Handles user questions and trouble reports
  - Maintains the token authentication database

- Provides temporary passwords for immediate access in case of lost/stolen/broken token

All the systems and processes ranging from provisioning to maintenance were tested and proven to support more than [redacted] users. The managed token service offers the Government the confidence in our ability to scale our service to meet Agency's needs with no learning curve and development.

Figure 1.6.7.1-1: AT&T Managed Subscription Token Service Architecture. *Agencies will receive a flexible token-based MEAS that offers a shared server environment for small Agencies and a dedicated server environment for large agencies.*

All communication to the authentication servers is restricted by managed firewalls. Firewall policies are implemented to allow access only by customer devices or AT&T system administrators. AT&T system administrators are limited to a small pool of AT&T users from a limited list of internal AT&T hosts.

The second service is a managed certificate offering. This service consists of a robust public key infrastructure (PKI), user administration, certificate authority (CA), 24x7x365 customer care, and management. **Figure 1.6.7.1-2** shows the AT&T PKI functional flow. Our PKI is deployed with the following functional capabilities:

- **Registration authority** – Support of electronic communications between the Government and the public for access to privacy information is dependent on the capability to authenticate applications and users. Users will receive electronic certificate after first proving their identify to the Registration Authority (RA).
- **Identification proofing** – Applying for a certificate requires verification of credentials that are provided by the public user for the purpose of receiving a certificate.
- **Certificate request** – The public user generates a public and private key pair and passes the public key to the RA. The RA requests a new certificate for the public user from the CA.
- **Certificate maintenance** – The RA will revoke, renew, or replace certificates as requested by the managed certificate offering.
- **Certificate authority** – Certificates are generated and maintained by the CA.
- **On-line certificate validation** – the CA will validate users before access is granted to information.

Figure 1.6.7.1-2: AT&T Functional Flow. *Agencies will receive MEAS from a [redacted] that is [redacted] with GSA offering services to Government Agencies.*

Both of our managed E-Authentication services are delivered using a proven approach of experienced personnel, certified processes, best-in-class tools, and high-touch client servicing. **Table 1.6.7.1-1** summarizes our service delivery approach.

SERVICE APPROACH	TECHNICAL DESCRIPTION
Standards compliance	We will offer MEAS that will comply with all applicable Federal, ITU, FIPS, NIST and IETF standards.
Design and engineering services	• Requirements collection, analysis, and documentation for baseline assessment • Trade studies that consist of equipment analysis, solution evaluation, and methods/procedures validation • Design and analysis of systems architecture, equipment, and configurations • Methods and procedures preparation • Security implementation and test plans
Account setup	• Setup user accounts for token card, key fob, and soft token • Provide user with password, pin number, and token device
AAA servers	• Design administration, authorization, and authentication (AAA) server architecture based on user requirements and performance thresholds • Provide AAA servers that are UNIX and Windows platforms that support remote authentication dial up service (RADIUS), terminal access controller access control system (TACACS), TACACS+, and DIAMETER • Implement and configure AAA servers in Government or AT&T facilities • Test and turn up AAA servers • Verify performance against key performance indicators (KPIs)
Implementation	AT&T well-established provisioning and service platform, which enables the Agency to quickly implement token authentication on their network(s) without the time delay to turn up and manage it themselves.
Managed [redacted] servers	• Interconnect AT&T data centers to Agency networks • Managed [redacted] servers per Agency • Remote authentication of users
Administration	• User account setup • User account move, add, change, and disconnect • Personal identification number (PIN) reset • Address changes and management • Management of tokens and other authentication devices
Management	AT&T will provide a fully managed, outsourced shared solution**,** or a managed custom solution will be configured to better suit Agency specific needs.
Customer Care	• AT&T Customer Care Center will offer a dedicated help desk or it will be integrated with a customer's existing support services. 24x7x365 customer care to end-users is also available on a toll-free number or a website. • Technical support for questions associated with the infrastructure is available during normal business days. Technical support for service-affecting problems associated with the infrastructure is available 24x7x365.

Table 1.6.7.1-1: Proven E-Authentication Service Delivery. *Agencies receive proven E-Authentication services that are delivered by experienced people, processes, tools, and client servicing.*

1.6.7.1.b Benefits to Technical Approach [L.34.1.6.1.b]

(b) Describe the expected benefits of the offeror's technical approach, to include how the services offered will facilitate Federal Enterprise Architecture objectives (see http://www.whitehouse.gov/omb/egov/a-1-fea.html). [L.34.1.6.1.a]

AT&T's Networx services support the Government's vision of transformation through the use of the Federal Enterprise Architecture (FEA) as a facilitating

mechanism to use technologies to contribute to mission performance. In describing services in relation to FEA, AT&T either summarizes its contribution or provides an example of how each service facilitates FEA implementation (**Table 1.6.7.1-2**). AT&T aligns its componentized products and services so they are easily integrated, commonly manageable, and usable across Government functions, horizontally and vertically, as well as between levels of Government. Security services, such as MEAS, are within the Technical Reference Model (TRM) and support the security management component of the FEA.

SERVICE DELIVERY APPROACH	BENEFITS	FEA FACILITATION
Design and engineering services	By using AT&T and our partners engineering and design experience Agencies will be able to collaboratively design MEAS solutions that integrate into their complex environment.	Authentication and E-Government
Administration	Agencies will benefit from receiving administrative services by allowing them to focus their efforts on Agency mission.	Authentication and E-Government
Token authenticators.	AT&T has used the same vendor token authentication technology internally to successfully safeguard its corporate network for years. We have tested and proven all the processes, from provisioning and customer support, to scaling the service, for more than 60,000 users.	Authentication and E-Government
Token authentication infrastructure	Shared servers provide two-factor authentication, central database storage, and administration of the token authentication service offering a high level of access security to Agencies.	Authentication and E-Government
Fully managed service	The Agency benefits from a comprehensive end-to-end managed service that includes full support, monitoring, and Service Level Agreements (SLAs).	System management and E-Government
Customer support help desk	AT&T provides 24 x 7 customer help desk support to assist Agencies with authentication questions/problems.	Forms management and E-Government
Integrated with other security services	Works with the secure managed email service (SMEMS) solution to help stop viruses before they enter the Agency's networks.	Security management and multiple components

Table 1.6.7.1-2: MEAS Delivery Approach Benefits. *Agencies will receive an authentication solution that has a proven track record of being stabile, reliable, and secure.*

From an FEA perspective, AT&T brings a market-based discipline, MEAS, which will support multiple lines of business (LoB) and subfunctions, as defined by the Business Reference Model (BRM). AT&T regards MEAS as a horizontal and

vertical capability of the Service Component Reference Model (SRM) that provides a component of security to the underlying communication infrastructure for individuals who need support or services from the Government.

AT&T's development of net-centric technologies supports solutions based on service-oriented architecture (SOA), which uses standardized, web-adapted components. Our approach incorporates the following criteria:

- Technical Reference Model capabilities are fully met and linked to the Service Component Reference Model (SRM) and Data Reference Model (DRM).
- These links are structured to support Business Reference Model (BRM) functions and provide line-of-sight linkage to mission performance and ultimate accomplishment per the Performance Reference Model (PRM)
- AT&T operates as an innovative partner through Networx to help achieve the vision of the FEA to enhance mission performance.

In addition to the benefits and FEA facilitations cited earlier, AT&T will assist specific departments and Agencies to meet mission and business objectives through a comprehensive MEAS offering.

1.6.7.1.c Major Issue to Service Delivery [L.34.1.6.1.c]

(c) Describe the problems that could be encountered in meeting individual service requirements, and propose solutions to any foreseen problems. [L.34.1.6.1.c]

In transitioning into any new service delivery model, whether it be task-based or fully outsourced, unforeseen issues can always arise. Therefore, it is important that GSA select a service provider that brings the depth and background to minimize an Agency's risk during transition. Our experience has enabled us to develop proven methods, processes, and procedures applicable to the simplest to the most complex projects.

Table 1.6.7.1-3 lists the top 6 service delivery risks and our mitigation strategy. As with all large, we enter each of these risks and others (after

identification and characterization) into our risk-tracking database and immediately take steps to mitigate them before they become an issue. Because risk management is more effective when all stakeholders are active in the process, AT&T engages the GSA, the client Agency, and other Government solution partners for success with risk mitigation activities.

RISK	DESCRIPTION	RISK MITIGATION
Business disruption	In our experience, all Agencies are concerned about business disruption when moving to a new service. Adequate planning will minimize this risk.	
Server sizing	When bringing on new customers or through organic growth, server capacity might be an issue.	
Jeopardy issues	All large projects encounter jeopardy issues during service delivery differences between quality provider and competitor in how they are handled.	
Loss of service	Server and appliance availability might be an issue.	
Interference	Updates and upgrades might interfere with Agency's daily schedule.	
Untimely administration	Requested changes to the system configuration might not be deployed in a timely fashion.	

Table 1.6.7.1-3: MEAS Service Delivery Lessons Learned and Risk Mitigation Strategies. *Agencies benefit from lessons learned and experience implementing MEAS services, which ultimately minimize service delivery risks.*

AT&T has taken steps to identify risk and provide risk mitigation associated with delivering MEAS. AT&T is committed to service excellence and will work with the Agency to identify and resolve potential problems that might occur during service delivery.

1.6.7.2 Satisfaction of Security Services Performance Requirements [L.34.1.6.2]

1.6.7.2.a Service Quality and Performance [L.34.1.6.2.a]

(a) Describe the quality of the services with respect to the performance metrics specified in Section C.2 Technical Requirements for each service. [L.34.1.6.2.a]

AT&T is committed to offering the Government the highest quality in MEAS; this commitment extends beyond simple promises. We offer the Government higher commitments than those offered in the commercial markets. **Table 1.6.7.2-1**lists our key performance indicators (KPIs) and acceptable quality levels (AQLs) for various service quality levels.

AT&T's confidence in our ability to deliver these performance results is supported by past performance and is backed by stringent service credits.

KEY PERFORMANCE INDICATOR	SERVICE LEVEL	PERFORMANCE STANDARD (LEVEL/THRESHOLD)	PROPOSED SERVICE QUALITY LEVEL
Grade of Service (Configuration Change)	Routine	Within 24 hours for a normal priority change	[redacted]
		Within 2 hours for an urgent priority change	
Event Notification (EN)	Routine	Within 4 hours of low category event	
		Within 30 minutes of high category event	
Time to Restore (TTR)	Without Dispatch	4 hours	
	With Dispatch	8 hours	
Availability	Routine	99.99% of the time	

Table 1.6.7.2-1: Performance Metrics for MEAS. *The Agency will receive quality e-authentication services that are supported by credit*

Focusing on an Agency's service experience produces a high-quality solution, and service experience must be measured quantitatively through the KPIs. However, high quality is not necessarily attained through exceptional performance of a single KPI. For example, an inferior response to the Agencies' maintenance and support needs can quickly erase the benefits of exceptional grade of service performance. Agencies will receive high-quality service through the combination of a production infrastructure that routinely goes through [redacted] and [redacted] audits. The Certificate

Authorities (CAs) are audited on a more frequent basis, sometimes as much as [redacted]

1.6.7.2.b Approach to Monitoring and Measuring Performance [L.34.1.6.2.b]

(b) Describe the approach for monitoring and measuring the Key Performance Indicators (KPIs) and Acceptable Quality Levels (AQLs) that will ensure the services delivered are meeting the performance requirements. [L.34.1.6.2.b]

Of equal importance to identifying the KPIs for a service is the method by which the KPIs are captured, measured, and monitored (**Table 1.6.7.2-2**). Agencies will receive the most accurate assessment of the service when the KPI measurement and monitoring methodology replicates the real performance that Agency personnel experience.

SERVICE APPROACH	TECHNICAL DESCRIPTION
Availability	[redacted]
Event Notification	[redacted]
Grade of Service	[redacted]
Time to Restore	[redacted]

Table 1.6.7.2-2: Managed Token Authentication Service Delivery Approach. *Agencies will receive a highly available service that has the tools and processes in place to monitor performance against delineated benchmarks.*

1.6.7.2.c Approach to Perform Service Delivery Verification [L.34.1.6.2.c]

(c) Describe the offeror's approach to perform verification of individual services delivered under the contract, in particular the testing procedures to verify acceptable performance and Key Performance Indicator (KPI)/Acceptable Quality Level (AQL) compliance. [L.34.1.6.2.c]

The first time the service is provided through the Networx contract, the service performance must be verified; KPIs will be monitored to certify that the service performance complies with the AQL. **Table 1.6.7.2-3** summarizes the verification and testing procedures for the MEAS KPIs.

SERVICE APPROACH	TECHNICAL DESCRIPTION
Availability	[redacted]
Event Notification	[redacted]
Grade of Service	[redacted]
Time to Restore	[redacted]

Table 1.6.7.2-3: Managed Token Authentication Service Verification Procedures. *Tools will be used to verify performance benchmarks and to assess compliance against contract requirements.*

To simplify the verification process, AT&T has automated the process. [redacted] The service verification process is presented in greater detail in Section 1.3.2.d, Approach to Perform Service Delivery Verification.

1.6.7.2.d Performance Level Improvements [L.34.1.6.2.d]

(d) If the offeror proposes to exceed the Acceptable Quality Levels (AQLs) in the Key Performance Indicators (KPIs) required by the RFP, describe the performance improvements. [L.34.1.6.2.d]

Achieving the AQLs defined by the Government for the Key Performance Indicators will result in superior MEAS service performance. [redacted]

1.6.7.2.e Approach and Benefits for Additional Performance Metrics [L.34.1.6.2.e]

(e) Describe the benefits of, and measurement approach for any additional performance metrics proposed. [L.34.1.6.2.e]

AT&T will provide weekly usage statistics (within the framework available with the vendor's authentication server product) showing authentication activity on an Agency-specific server. These statistics include allowed secure accesses, denied secure accesses, new authentication users added during a specific timeframe, total number of users, and total number of managed tokens per Agency-specific server. Using these statistics, the Agency can chart usage and growth of the authentication service and plan for future needs accordingly and can be the basis on additional KPIs on a task order basis.

1.6.7.3 Satisfaction of Security Services Specifications [L.34.1.6.3]

1.6.7.3.a Service Requirements Description [L.34.1.6.3.a]

(a) Provide a technical description of how the service requirements (e.g., capabilities, features, interfaces) are satisfied. [L.34.1.6.3.a]

1.6.7.3.a.1 Capabilities and Features of Managed Token

MEAS is part of our overall security solution portfolio that includes multi-layered security environment, designing security into the network and services, focusing on methods and systems to enhance security, and to respond to and mitigate incidents. Transferring our own proven security innovations to the Agency further extends the multilayered security approach. The Agency is provided with a fully managed, outsourced shared solution, or a managed custom solution is configured to better suit its specific needs. These service options allow the Agency to concentrate on the need to conduct transactions with the well-established provisioning and service platform, which enables the Agency to quickly implement Token Authentication on its networks without the time delay to turn up and manage it themselves.

The Agency can benefit from our long history in developing, supporting and deploying information security services to meet the demanding requirements of the U.S. Government and our corporate customers. **Table 1.6.7.3-1** lists the token authentication service capabilities and features in support of Agency users remotely authenticating their identities to an Agency IT system.

SERVICE REQUIREMENTS	DESCRIPTION	BENEFITS TO AGENCY
Shared solution	[redacted]/Servers are owned and managed by AT&T, physically located in [redacted] and accessed by Agency and its users via the Internet.	Agencies will receive a cost benefit from receiving MEAS in a shared environment.
Dedicated solution	Customer may use one or more AT&T-owned [redacted]/Servers, dedicated to Customer. Alternatively, Customer may purchase [redacted]/Servers from AT&T. The Dedicated Solution options include: engineering services, collocation, and redundancy options.	Agencies will receive a flexible solution from receiving MEAS in a dedicated environment.
Design and engineering services	• Requirements collection, analysis, and documentation for baseline assessment [redacted] • Design and analysis of systems architecture, equipment, and configurations • Methods and procedures preparation • Security implementation and test plans	By using AT&T and our partners engineering and design experience Agencies will be able to collaboratively design MEAS solutions that integrate into their complex environment.
Implementation	AT&T well-established provisioning and service platform, which enables the Agency to quickly implement token authentication on their network(s) without the time delay to turn up and manage it themselves.	Agencies will benefit from receiving implementation services by allowing them to focus their efforts on Agency mission.
Token authentication server	The server controls the user-authentication aspect of the service, using a central database for administration of user accounts and security policies.	Shared servers provide two-factor authentication, central database storage, and administration of the token authentication service.
Token authentication agents	Agents provide the interface for users desiring access to protected resources to enter passwords and token codes. Agents are device-specific software built into protected network equipment on the customer's premises. Agents can also use [redacted] software that can be installed onto web servers, domain servers, or other servers. Agents can also use custom-written software to support the Agency's applications with the vendor's application programming interface (API). The products of more than 140 leading vendors of firewalls, remote access servers, virtual private networks (VPNs), and web applications support two-factor authentication right from the box, so it is likely the agents are already in place.	A standards based system easily integrates with standard [redacted] promoting interoperability.
Token authenticator	An authenticator is a small, user-carried key fob device. Each authenticator contains a unique [redacted] that is combined with a powerful algorithm to generate a new code every [redacted]. Because the number is unpredictable and dynamic, it would be extremely difficult for a hacker to guess the correct number at any given time. Patented technology synchronizes each authenticator with the token authentication server, providing a high level of security.	AT&T has used the same vendor token authentication technology [redacted] to successfully safeguard [redacted]. We have tested and proven all the processes, from provisioning and customer support, to scaling service for more than [redacted] users.

SERVICE REQUIREMENTS	DESCRIPTION	BENEFITS TO AGENCY
Token authentication customer care center	The Customer Care Center provides customer support and administers the service, including the following tasks: • Distributes and replaces token authenticators to users • Provides Internet accessible, web-based self-help tool for all token requests • Maintains token authentication database • Provides temporary passwords for immediate access in case of lost/stolen/broken token on a self-help web-based interface • Allows ability to submit trouble tickets on self-help, web-based interface	AT&T provides customer help desk support to assist users with authentication questions/problems.

Table 1.6.7.3-1: Managed Token Authentication Service. *Agencies will receive a managed solution that offers the flexibility to meet Agencies demanding security needs.*

Figure 1.6.7.3-1 outlines the Token Authentication (TA) process step-by-step. If the user experiences a problem, the Customer Care Center can be contacted via e-mail or telephone to request help.

1. A user initiates access via the Internet to a TA-enabled corporate resource – for example, VPN, Microsoft Exchange Mail Server, intranet. The service supports several modes of Internet access including dial-up, DSL, cable modem, dedicated for example, T-1, and wireless-enabled devices, such as those using 802.11b / WiFi, GPRS, CDPD technologies.
2. The company requests the and
3. Using the , the user reads and enters the and also enters the
4. The forwards the user's and to the
5. The the and for the corporate resource against the TA database and provides the results to the
6. The or the user to the corporate resource, based on these results.
7. If authorized, the user

Figure 1.6.7.3-1 The *The supports the Agency's need for developing, implementing, and maintaining a*

1.6.7.3.a.2 Capabilities and Features of Certificate-Based Services

AT&T offers Agencies a certificate-based service that will provide the citizen and Agencies the ability to authenticate applications and transaction. The service is intended to provide identification, authentication, and non-repudiation through the use of digital signature technology as a means for individuals, businesses, and Agencies to be authenticated when accessing, retrieving, and submitting information.

AT&T's certificate-based MEAS provides the following capabilities and features in support of the Agency's need for a person to remotely authenticate his identity to an Agency IT system (**Table 1.6.7.3-2**).

SERVICE REQUIREMENTS	DESCRIPTION	BENEFITS TO AGENCY
Design and engineering services	• Requirements collection, analysis, and documentation for baseline assessment • Trade studies that consist of equipment analysis, solution evaluation, and methods/procedures validation • Design and analysis of systems architecture, equipment, and configurations • Methods and procedures preparation • Security implementation and test plans	[redacted]
Implementation	AT&T well-established provisioning and service platform, which enables the Agency to quickly implement token authentication on their network(s) without the time delay to turn up and manage it themselves.	[redacted]
Public key infrastructure	AT&T will provide a production a public key infrastructure that will provide all the functionality required to authenticate users; SSL equipped servers, database w/ user names, Ids, and passwords; and directory and repository.	Agencies will receive a proven production PKI that supports Government agencies today.
[redacted]	AT&T will provide the [redacted] function that will [redacted] to [redacted] after [redacted] the [redacted]	Agencies will be provided this critical certificate based MEAS function as part of our standard service enabling them to be digitally authenticated with ease.
Identification proofing	[redacted]	
Certificate authority	AT&T will provide the certificates that are generated and maintained by the Certificate Authority.	

SERVICE REQUIREMENTS	DESCRIPTION	BENEFITS TO AGENCY
Certificate administration and maintenance	The RA will revoke, renew, or replace certificates as requested by the user.	By allowing AT&T to provide administration and maintenance of this MEAS Agency users will be provided an easy to use interface.
Online certificate validation	The CA will validate users before access is granted to information.	Online certificate validation provides an electronic capability for validation.
Interoperability	Certificates issued the CA will be interoperable with all Government Agencies applications.	Interoperability provides ease of integration of MEAS into an Agencies information technology infrastructure.
Certificate-based Customer Care Center	The Customer Care Center provides customer support and administers the service.	AT&T provides customer help desk support to assist users with authentication questions/problems.

Table 1.6.7.3-2: Managed Certificate Based Authentication Service. *Agencies will receive a managed solution that offers the flexibility to meet Agency's demanding security needs.*

1.6.7.3.a.3 Registration Authority and Identity Proofing

AT&T has extensive experience registering and validating individuals and organizations that use a wide variety of AT&T services everyday. Based on this experience, AT&T has created a Registration Authority (RA) that is secure, easy to use, well-documented, and fully supported to all individuals, business representatives, and Agency applications. The AT&T RA provides the means and the support for all certificate applicants to perform the following tasks:

- Successfully generate their public and private key pair
- Request, retrieve, and install their certificate
- Suspend, revoke, renew, or replace their certificate.

The AT&T RA also interfaces with an Identity Proofing Agent (IPA) to validate the identities and business of all potential subscribers.

1.6.7.3.a.4 Certificate Issuance and Delivery

Upon receipt of a certificate request, the AT&T CA will digitally sign the applicant's certificate request to create an digital certificate and store it in its certificate repository. The AT&T CA will send a notification message to the AT&T RA to inform it that the applicant's certificate is available. The AT&T RA will send a letter to the applicant by postal mail to inform him that his

certificate is ready to be retrieved. The letter will also include a copy of the applicant's parsed certificate, the universal resource locator (URL) to retrieve the certificate, and a PIN.

The applicant will establish an Internet connection, launch his web browser, and establish an authenticated and private communication link with AT&T RA's website by following the URL in the letter. All applicants will be presented with a web form that requires them to acknowledge the following items before they can retrieve their certificate:

- The applicant will use the certificate exclusively for purposes of authentication of identity, enabling access to Agency applications for electronic information and transactions.
- The applicant will instruct AT&T to revoke a certificate when no longer needed.
- The applicant will instruct AT&T to revoke the certificate promptly upon any actual or suspected loss, disclosure, or other compromise of the subscriber's private key.
- The applicant will respond, as required, to notices issued by the contractor.
- The applicant will acknowledge that AT&T will revoke the certificate if the subscriber does not meet these responsibilities.

Upon accepting the above statements, the applicant will be directed to another web form where he enters the PIN that was in the letter he received. When the applicant hits the *submit* button, his PIN is sent to the AT&T RA for verification. If the PIN is not verified, the AT&T RA asks the applicant to verify his PIN and re-submit it to the AT&T RA. The applicant is directed to Customer Service for assistance if he fails to enter the

correct PIN after three attempts. If the applicant's PIN was verified by the AT&T RA, the AT&T RA obtains the applicant's certificate from AT&T CA certificate repository and transmits it to the applicant's web browser.

UNDERLYING NETWORX OFFERING	MNS SUPPORTED
Frame Relay	✓
ATM	✓
Internet Protocol (IP)	✓
NBIPVPN	✓
PBIPVPN	✓

Table 1.6.7.3-3: Transport Services available for MEAS. *Available to the Agencies are a variety of transport service options to build their unique MEAS solution.*

1.6.7.3.a.5 Interfaces

In accordance with the RFP, the MEAS connects and interoperates with underlying Networx offerings (**Table 1.6.7.3-3**).

1.6.7.3.b Attributes and Values of Service Enhancements [L.34.1.6.3.b]

(b) If the offeror proposes to exceed the specified service requirements (e.g., capabilities, features, interfaces), describe the attributes and value of the proposed service enhancements. [L.34.1.6.3.b]

AT&T will provide, test, and deploy vendor-supplied application security and/or functionality enhancements and upgrades to the authentication service as they become available to AT&T. AT&T will maintain and enhance the customer self-help web service provided as part of the managed token service.

1.6.7.3.c Service Delivery Network Modifications [L.34.1.6.3.c]

(c) Describe any modifications to the network required for delivery of the services. Assess the risk implications of these modifications. [L.34.1.6.3.c]

Agencies receive a low-risk solution through AT&T's ability to offer MEAS upon contract award without modifications to the network or operational support systems.

1.6.7.3.d Security Services Experience [L.34.1.6.3.d]

(d) Describe the offeror's experience with delivering the mandatory Security Services described in Section C.2 Technical Requirements. [L.34.1.6.3.d]

Agencies are offered extensive MEAS experience that creates value to our customers to both in Government and commercial entities. This experience

has given us the ability to engineer and deliver services. Two examples of AT&T Team's ability to deliver MEAS are listed in **Table 1.6.7.3-4**.

[redacted]

AT&T NEED	SOLUTION	CREATE VALUE
[redacted]	[redacted]	[redacted]

AT&T NEED	SOLUTION	CREATE VALUE
[redacted]	[redacted]	[redacted]

Table 1.6.7.3-4: Service Experience. *AT&T has an extensive history in providing MEAS to commercial and Government customers as well as protecting their own vast infrastructure.*

1.6.7.4 Stipulated Deviations

AT&T takes neither deviation nor exception to the stipulated requirements.