

### 6.2.3 Managed E-Authentication Service (MEAS) (L.34.1.6.4, M.2.1.3)


*The Qwest Team's MEAS provides a fully outsourced and tightly integrated solution of authentication technologies including tokens, digital certificates, biometrics, and software encryption.*

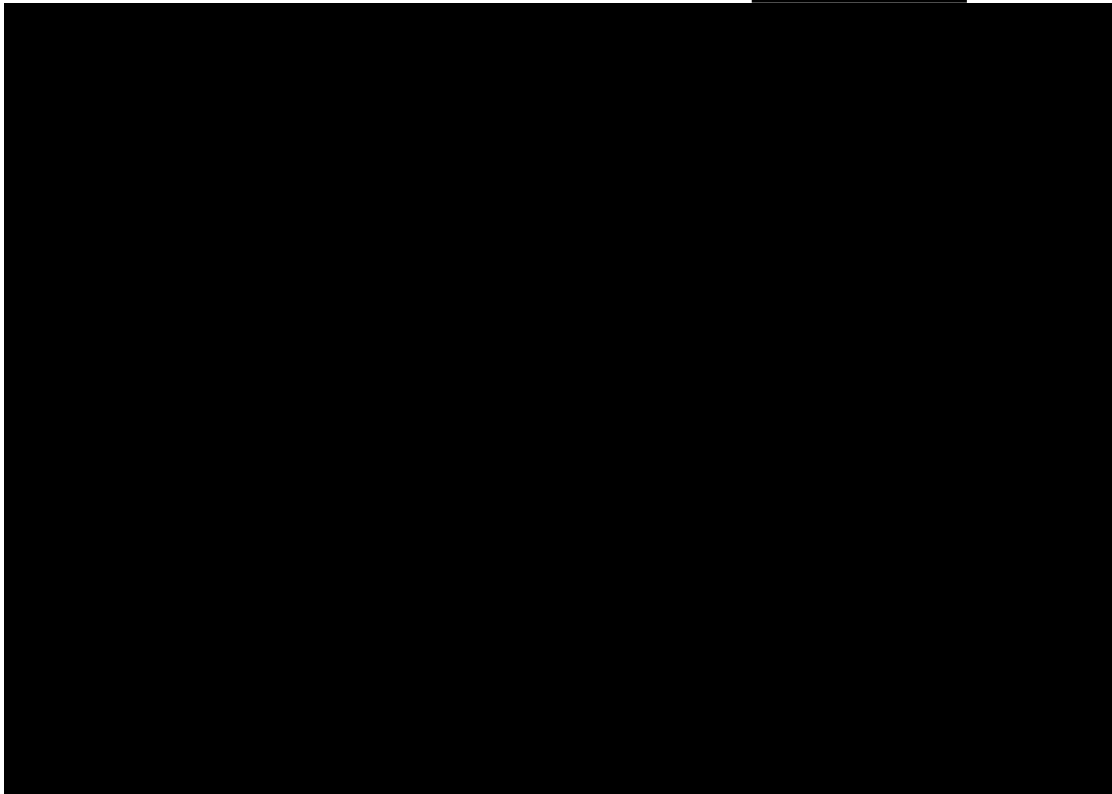
Qwest has teamed [REDACTED] to provide Agencies with security services to fulfill the requirements of the RFP.

The Qwest Team's Managed E-Authentication Service (MEAS) provides design, implementation, and operational capabilities for both token-based and certificate-based E-Authentication services in a variety of Agency environments. The Qwest Team offers significant capabilities in identity management, access control, and biometrics. Our service is provided by a unique and tightly integrated combination of services from our teammates [REDACTED]. Our service is available globally and supports connectivity via the Internet, Agency de-militarized zones, and secure Local Area Networks. The Qwest Team's MEAS capability offers optional services to meet additional Agency needs, such as key management, roaming, and premium validation services. [REDACTED]

[REDACTED]

The Qwest Team provides the primary connectivity between users, servers, and the E-Authentication infrastructure as well as the necessary user interfaces. The Qwest Team provides secure network transport solutions to the E-Authentication service. [REDACTED] engineers and manages the E-Authentication service including biometric authentication, user databases, and service data. [REDACTED] provides the back-end services, such as certificate

authorities and registration authorities. These components are tightly integrated so that a user is presented with a cohesive service. The E-Authentication system infrastructure is depicted in 



**6.2.3.1 Reserved (L.34.1.6.4 (a))**

**6.2.3.2 Reserved (L.34.1.6.4 (b))**

**6.2.3.3 Technical Service Requirements (L.34.1.6.4 (c))**

The Qwest Team's MEAS offering is a fully integrated enterprise solution designed to secure intranet, extranet, and Internet applications. MEAS enables fluid interaction with business partners, mobile workers, Web service devices, and other users. This highly scalable service allows Agencies to rapidly establish a robust Public-Key Infrastructure (PKI) and Certificate Authority (CA) system while avoiding the burden of PKI deployment, maintenance, and oversight. Agencies retain complete control

over security policy, authentication models, and certificate lifecycle/certificate revocation management.

Built on open standards to ensure maximum flexibility, our MEAS allows interoperability with virtually any application or device and is integrated with leading commercial-off-the-shelf technology, including Microsoft applications and Windows operating systems. By leveraging the MEAS to deploy digital certificate services, Agencies can reduce the cost and complexity of PKI implementations while providing globally trusted, state-of-the-art authentication, encryption, digital signing, and non-repudiation services.

**6.2.3.3.1. Satisfaction of MEAS Capability Requirements (L.34.1.6.4 (c), C.2.10.6.1.4)**

The 20 MEAS technical capabilities shown in **Figures 6.2.3-2** through **6.2.3-6** are essential to achieving an effective service and high degree of Agency satisfaction. The Qwest Team meets all requirements and works closely with Agency organizations to design, implement, and operate the MEAS in accordance with their requirements.

Qwest fully complies with all mandatory stipulated and narrative capabilities requirements for MEAS. The text in Figure 6.2.3-2 provides the technical description required per L.34.1.6.4 (c) and does not limit or caveat Qwest's compliance in any way.

**Figure 6.2.3-2. Qwest Team MEAS Design and Engineering Capabilities**

MEAS Design and Engineering Capabilities	[Redacted]
<p>E-Authentication networking infrastructure design and engineering services meet Agency requirements. Services include, but are not limited to system architecture and equipment recommendations, a baseline assessment, a final design configuration, and operational procedures.</p>	[Redacted]
<p>The contractor shall support the Agency in developing detailed plans for implementation of user authentication service. The contractor shall offer to provide installation and integration support to the Agency, including but not limited to testing of equipment and software, cost information, and loading of customer-relevant data.</p>	[Redacted]

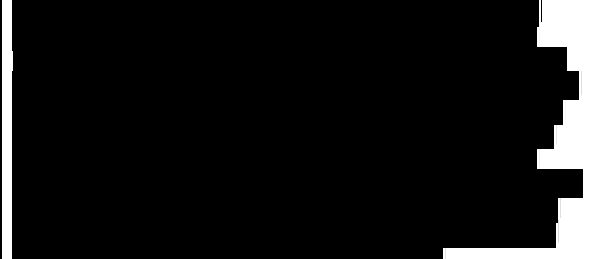
**Figure 6.2.3-3. Qwest’s Token-Based Implementation Capabilities**

MEAS Token-Based Implementation Capabilities	[Redacted]
<p>1. The contractor for the managed PKI service shall set up the authentication service at the identity authentication assurance level specified by the Agency and issue smart cards and/or other token devices in the quantities needed by an Agency, including:</p> <ul style="list-style-type: none"> <li>a. Token Card with or without Password and Personal Identification Number (PIN)</li> <li>b. Key Fob</li> <li>c. Soft Token</li> </ul>	[Redacted]
<p>2. The service shall follow the E-Authentication federated authentication model to allow Agencies to validate multiple levels of authentication via a single interface and enable inter-Agency acceptance of digital certificates and single sign-on capability.</p>	[Redacted]

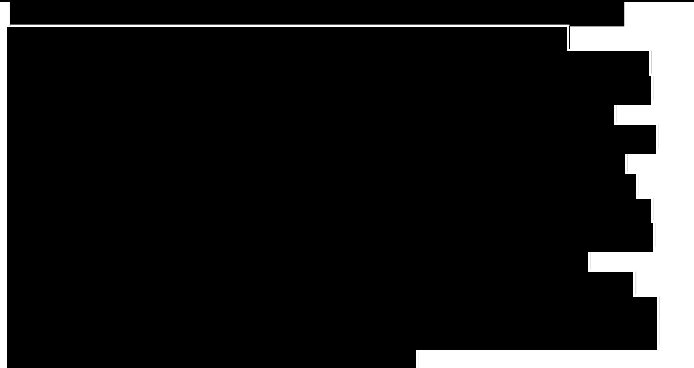
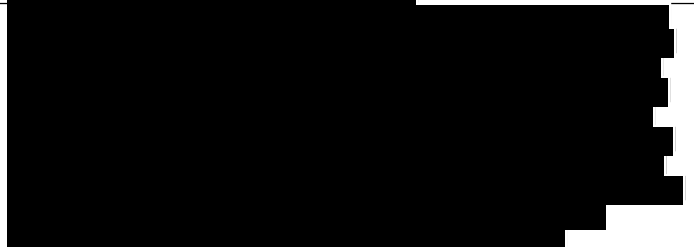


MEAS Token-Based Implementation Capabilities	
3. The contractor shall support the Agency-specified user ID naming scheme to meet Agency requirements.	[REDACTED]
4. Implement Secure Sockets Layer (SSL) and/or Transport Layer Security (TLS) equipped servers as well as appropriate acceleration capabilities as required by the Agency to meet Agency performance requirements.	[REDACTED]
5. Provide methods including but not limited to the following as needed by the Agency. <ul style="list-style-type: none"> <li>a. Password and Personal Identification Number (PIN)</li> <li>b. Authentication Methods based on Fingerprints.</li> <li>c. Network Authentication Systems and Servers for Embedded Devices (for example, routers, modem servers, and switches)</li> </ul>	[REDACTED]
6. Contractor shall support in developing, implementing, and maintaining the Authentication, Authorization and Accounting (AAA) system and servers for network access, including the related tokens, based on but not limited to: <ul style="list-style-type: none"> <li>a. Remote Authentication Dial-In User Service (RADIUS)</li> <li>b. TACACS/TACACS+(Cisco)</li> <li>c. Diameter</li> </ul>	[REDACTED]

**Figure 6.2.3-4. Qwest’s Token-Based Management Capabilities**

MEAS Token-Based Management Capabilities	
1. Manage and maintain the user authentication service including related tokens, such as but not limited to: <ul style="list-style-type: none"> <li>a. One-Time Passwords</li> <li>b. Smart Cards</li> <li>c. Hardware Tokens</li> </ul>	[REDACTED]
2. Provide change management functions of the authentication service as requested by Agency designated points of contact (POCs), including but not limited to: <ul style="list-style-type: none"> <li>a. Adding a New User</li> <li>b. Deleting a Current User</li> <li>c. Resetting the PIN</li> <li>d. Changing, Adding, or Deleting IP Addresses of Software Agent</li> <li>e. User ID Administration</li> </ul>	[REDACTED]

MEAS Token-Based Management Capabilities	
<p>3. Ensure uninterrupted operations using mechanisms such as redundant servers that are located in geographically separate locations with the content continuously synchronized between them.</p>	

**Figure 6.2.3-5. Qwest MEAS Certificate-Based Implementation Capabilities**

MEAS Certificate-Based Implementation Capabilities	
<p>1. Manage PKI that comprises but is not limited to CA, Registration Authority, Directory, and associated servers.</p>	
<p>2. The contractor shall host and administer PKI certificates for an Agency, including but not limited to certificate issuance, validation services, Agency application certificate registration, and management.</p>	
<p>3. The contractor for the managed PKI service shall set up the authentication service at the identity authentication assurance level specified by the Agency and issue digital certificates in the quantities needed by an Agency.</p>	
<p>4. The service shall follow the E-Authentication federated authentication model to allow Agencies to validate multiple levels of authentication via a single interface and enable inter-Agency acceptance of digital certificates and single sign-on capability.</p>	

MEAS Certificate-Based Implementation Capabilities	[Redacted]
<p>5. The contractor shall establish a networking environment that provides the communication among PKI elements, including but not limited to CA. The contractor shall implement secure sockets layer (SSL) and/or transport layer security (TLS) equipped servers as well as appropriate acceleration capabilities as required by the Agency to meet Agency performance requirements.</p>	<p>[Redacted]</p>

**Figure 6.2.3-6. The Qwest Team’s Certificate-Based Management Capabilities**

MEAS Certificate-Based Management Capabilities	[Redacted]
<p>1. The contractor for the managed PKI service shall maintain the database of: a. User Names b. User IDs c. Passwords</p>	<p>[Redacted]</p>
<p>2. The contractor shall provide digital certificates and digital signatures within PKI as well as CA services.</p>	<p>[Redacted]</p>
<p>3. The contractor shall ensure uninterrupted operations using mechanisms such as redundant servers that are located in geographically separate locations with the content continuously synchronized among them.</p>	<p>[Redacted]</p>
<p>4. The contractor shall provide change management functions of the managed PKI service, as requested by Agency-designated POCs, including but not limited to: a. Adding a New User b. Deleting a Current User c. Resetting the Password d. Changing, Adding, or Deleting IP Addresses of Software Agent e. User ID Administration</p>	<p>[Redacted]</p>

**6.2.3.3.2 Satisfaction of MEAS Features Requirements (L.34.1.6.4 (c), C.2.10.6.2)**

Qwest fully complies with all mandatory stipulated and narrative features requirements for MEAS. The text in **Figure 6.2.3-7** provides the technical description required per L.34.1.6.4 (c) and does not limit or caveat Qwest’s compliance in any way.

**Figure 6.2.3-7. Qwest Team MEAS Required Features**

ID #	Name of Feature	Description	
1	Biometric Characteristics	The contractor shall provide biometric authentication methods, including iris scan, voice, and facial recognition, as required by the Agency.	[REDACTED]
2	Encryption / Digital Signature Client Software	The contractor shall provide and support the encryption/digital signature client software for the Agency-designated POCs.	[REDACTED]
3	E-Authentication Training	The contractor shall provide E-Authentication training to Agency personnel as required. This includes but is not limited to user authentication, PKI, and CAs. The frequency and nature of training activities may vary according to Agency needs.	[REDACTED]
4	Directory/ Repository Function	The contractor shall develop, implement, and maintain a directory/repository function that will support the PKI and/or other E-Authentication mechanism chosen by the Agency.	[REDACTED]

**6.2.3.3.3 Satisfaction of MEAS Interface Requirements (L.34.1.6.4 (c), C.2.10.6.3)**

Qwest provides all mandatory and optional interfaces based on the capabilities of Qwest’s proposed services as defined in Frame Relay Service (Proposal Section 4.2.3), Asynchronous Transfer Mode Service (Proposal Section 4.2.4), Internet Protocol Service (Proposal Section 4.1), Premises-Based IP Virtual Private Network (VPN) Services (Proposal Section 4.2.8), and Network-Based Internet Protocol VPN (Proposal Section 4.1.2). Qwest fully complies with all mandatory stipulated and narrative features requirements for MEAS. The texts in the above-referenced sections provide the technical description required per L.34.1.6.4 (c) and do not limit or caveat Qwest’s compliance in any way.

**6.2.3.4 Achieving Quality of Service Goals (L.34.1.6.4 d)**

The Qwest Team’s MEAS meets all performance requirements, summarized in **Figure 6.2.3-8**. We have proven monitoring and measurement systems, procedures, and evaluation methods in place. The Government's required performance measures are synchronized with commercial standards, and we are prepared to meet each of these performance requirements.

**Figure 6.2.3-8. Qwest Team MEAS Key Performance Indicators (KPIs)**

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	
Availability	Routine	99.99%	≥ 99.99%	
Event Notification (EN)	Routine	Within 4 hours of a Low category event (Severity 2 or 3)	≤ 4 hours	
		Within 30 minutes of a High category event (Severity 1)	≤ 30 minutes	
Grade of Service (Configuration Change)	Routine	Within 24 hours for a Normal priority change (Severity 2 or 3)	≤ 24 hours	
		Within 2 hours for an Urgent priority change (Severity 1)	≤ 2 hours	
Time To Restore (TTR)	Without Dispatch	4 hours (Severity 1)	≤ 4 hours	
	With Dispatch	8 hours (Severity 1)	≤ 8 hours	

**Availability:** The Qwest Team's MEAS meets Availability Acceptable Quality Levels (AQLs) because it is delivered through industry-leading technology platforms. The servers and systems providing MEAS are designed for redundancy and scalability on carrier-class hardware. This architecture includes fully-redundant data centers in different geographic locations with clustered servers, redundant power, and synchronized databases [REDACTED]

[REDACTED] Our MEAS incorporates no single point of failure that can disrupt production operations.

[REDACTED]

**Event Notification (EN):** Our proactive network monitoring capabilities correlate network performance statistics and trigger performance thresholds, which automatically create notification trouble tickets [REDACTED]

[REDACTED] Threshold levels are established to correspond with low ( $\leq 4$  hours) and high category ( $\leq 30$  minutes) events, which are also communicated to the Agency.

**Grade of Service (Configuration/Change):** Configuration changes are input by the Agency via the Qwest Control Network Portal. Changes initiated by the Qwest Team require Agency consent prior to implementation. Changes are categorized as Normal and Urgent (Emergency). [REDACTED]

[REDACTED]

[REDACTED] Agency administrators can make certain Grade of Service changes



[Redacted text block containing multiple paragraphs of blacked-out content]

**6.2.3.6 The Qwest Team's Experience – Delivery of Matching Service Capabilities (L.34.1.6.4 (f))**

[REDACTED]

[REDACTED] E-Authentication services are delivered through our [REDACTED] PKI and SOC, ensuring 24x7x365 monitoring, management, and escalation across the globe. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

**6.2.3.7 Approach to Performance Verification (L.34.1.6.4 (g))**

Our MEAS AQL compliance is verified through a combination of internal audit, test and verification processes, trouble ticket records, and executive summary reports. An executive dashboard report provides an interactive summary of the overall MEAS performance, complete with graphs, performance statistics, threat levels, Help Desk summaries, and vulnerabilities by service level. Determining availability based upon alarms (and associated trouble tickets) is the normal and least intrusive approach used. At the end of each evaluation period, availability and TTR will be calculated, and AQL performance reports will be available to Agencies

[REDACTED]

To ensure AQLs are met and that critical issues are immediately addressed, thresholds are set depending on the nature of the event. The events are tracked via individual tickets that are prioritized based on classification and response time AQLs. Performance levels are monitored

[REDACTED]

[REDACTED]

[REDACTED] in order to ensure monitoring accuracy and maintain a profile of Agency information security posture [REDACTED]

[REDACTED]

The ticket is subsequently tracked and updated for technical and AQL performance throughout the escalation process until successful closure. Verification of MEAS requires extensive interaction and proactive monitoring capabilities combined with the expert knowledge of the Qwest Team's SOC-certified security professionals. Our ability to identify events, perform triage, and respond meets the Agency's AQL requirements.

Qwest will provide all necessary monitoring as part of the service. The SOC lead engineer assigned to the Agency is responsible for monitoring and oversight of the performance of the Service Level Agreement after the service has been implemented. The Qwest Team's delivery experience, combined with our knowledge that each Agency will have unique requirements, especially around GoS, allows the definition of appropriate change control processes and commitment levels by task order AQLs.

**6.2.3.8 Service Impact to Network Architecture (L.34.1.6.4 (h))**

Traffic generated by monitoring and telemetry functions related to MEAS represents an insignificant impact to the Qwest Network. The architecture of our MPLS-based transport layer accommodates connectivity to security platforms as an element of standard design.

**6.2.3.9 Approach to Satisfying NS/EP Requirements (L.34.1.6.4 (i))**

As defined in RFP Section C.5.2.2.1, MEAS is not an NS/EP-impacted service. Qwest's overall support of the NS/EP requirements can be found in Section 3.5.1, and our NS/EP plan can be found in Appendix 2 to the Technical Volume.

**6.2.3.10 Approach to Assured Service in the National Capital Region  
(L.34.1.6.4 (j))**

Qwest is currently a leading provider of network services in the National Capital Region (NCR) with robust network architecture to ensure service continuity in the event of significant facility failures. Qwest continues to engineer critical services to meet the requirements of each customer eliminating single points of failure for their network services.

Qwest understands the Government's requirement to assure performance of network services in and around the NCR. To meet this important requirement, Qwest has established Point-of-Presence (POP) diversity in the NCR. [REDACTED]

[REDACTED] Each of these gateways provides complete redundancy to access Qwest nationwide and international network capabilities as well as regional voice and data services. [REDACTED]

[REDACTED]

Qwest has recently acquired OnFiber, a metro SONET and Ethernet provider with yet another diverse network in the NCR. [REDACTED]

[REDACTED] Section 3.5.2 provides further information describing Qwest's NCR infrastructure.

The Qwest Team has multiple SOCs that are geographically diverse, and no Managed Security Service is dependant on assets located solely within the NCR region.

**6.2.3.11 Approach to Meeting Section 508 Provisions (L.34.1.6.4 (k))**

Qwest's approach to Section 508 provisions is to ensure that all Agency users are able to access all systems and services. To ensure this, the Qwest Control Network Portal will be 508 compliant. The Qwest Control

Networkx Portal is the gateway to Qwest Networkx support systems, serving as the primary conduit for daily status pertaining to ongoing projects and other service delivery activities for Agencies. The support systems for MEAS are compliant with applicable accessibility standards in Subpart B.

In addition, Qwest has enlisted a toll-free number for 24x7x365 access, 1-866-GSA-NETWorx (1-866-472-6389), which will allow domestic Agency users to have access to our Customer Support Office, which will also be 508 compliant—enabling access by email, fax, Telecommunications Display Device, text messaging, or other methods as required. Qwest customer service support will be accessible around the clock for all Agency users, wherever they may be located.

[REDACTED]

**6.2.3.12 Approach to Incorporating Technological Enhancements and Improvements (L.34.1.6.4 (I))**

Qwest has a proven, mature process that enables us to envision, research, evaluate, engineer, deploy, and operate new or emerging services, including MEAS. Driven initially by the Chief Technology Office, Qwest evaluates new products and technologies for incorporation into the Qwest network in partnership with Qwest Product Management.

[REDACTED]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[REDACTED]

Qwest's suppliers participate fully in this process. Qwest ensures compliance with suppliers by evaluating, testing, and certifying all emerging technology. The vendors on the Qwest Team are committed to driving new technologies and products. New technology provided by suppliers is also driven through and implemented via the NTSC process in order to standardize all new products and technologies we will present to Agencies.