

## Appendix

Included in the following pages is the current draft of the E-Authentication Federation's "Business Rules: E-Authentication Federation."

Version 1.0

November 23, 2004

FINAL DRAFT

Written by [Daniel Greenwood](#), Esq., with Input from Linda Elliott and RJ Schlecht

## E-Authentication Business Rules Table of Contents

1. <b>Title</b> .....	1
2. <b>Scope</b> .....	1
2.1. Scope of Rules .....	1
2.2. Agreements and Conduct Outside Scope of Rules .....	1
2.3. Rules Appearing in Multiple Documents .....	1
3. <b>Participation</b> .....	1
3.1. Eligibility .....	1
3.2. Participation Requirements .....	1
3.2.1. Relying Parties .....	1
3.2.2. CSPs .....	1
3.2.3. End-Users .....	2
4. <b>Roles and Obligations</b> .....	2
4.1. GSA Role and Obligations .....	2
4.1.1. Operating Authorization .....	2
4.1.2. Promulgation and Amendment of Business Rules and Other Documents .....	2
4.1.3. Relying Party and CSP Approval .....	3
4.1.4. Service Offerings .....	3
4.1.4.1. Architectural Components .....	3
4.1.4.2. Interoperability Requirements .....	3
4.1.5. Contact Information .....	3
4.2. Relying Party Role and Obligations .....	3
4.2.1. Relying Party Participation Agreement .....	3
4.2.2. Interface Specification, Approved Software Use and Upgrade .....	3
4.2.3. Security and Privacy Compliance .....	4
4.2.4. Reasonable Reliance and Level of Assurance .....	4
4.3. CSP Role and Obligations .....	4
4.3.1. CSP Certification .....	4
4.3.2. CSP Participation Agreement .....	4
4.3.3. CSP Continuing Audit Requirement .....	4
4.3.4. Material Change to CSP, Credential Services or Credential .....	5
4.3.5. Interface Specification .....	5
4.3.6. End-User Notice Terms .....	5
4.4. General Obligations .....	5
4.4.1. Record Keeping .....	5
4.4.2. Federation Security and Reliability .....	5
4.4.3. Federation Interoperability .....	6
4.4.4. Operational and Ongoing Requirements .....	6
4.4.5. Authentication of Approved Parties .....	6
4.4.6. End-User Privacy .....	6
5. <b>Enforcement</b> .....	6
5.1. Dispute Resolution .....	6
5.2. GSA Investigation .....	7
5.2.1. Federation Participant Request for Investigation .....	7
5.2.2. GSA Initiated Investigation .....	7
5.3. Recourse .....	7
6. <b>General Legal Terms</b> .....	7
6.1. Limitation Of Liability .....	7
6.2. Governing Law .....	7

6.3. Order of Precedence. . . . .	7
6.4. Assignment, Succession and Bankruptcy. . . . .	8
6.5. Severability. . . . .	8
6.6. Counterparts. . . . .	8
6.7. Waiver . . . . .	8
6.8. Responsibility For Taxes, Expenses. . . . .	8
<b>7. Interpretation and Amendment. . . . .</b>	<b>8</b>
<b>Appendix 1. CSP Participation Agreement. . . . .</b>	<b>9</b>
<b>Appendix 2. Relying Party Participation Agreement. . . . .</b>	<b>11</b>
<b>Appendix 3. Business Rules Amendment Process. . . . .</b>	<b>13</b>
<b>Appendix 4. General Overview. . . . .</b>	<b>14</b>
<b>Appendix 5. Glossary. . . . .</b>	<b>17</b>
<b>Appendix 6. Endnotes. . . . .</b>	<b>19</b>

**Drafting Notes:**

This document complies with the following drafting conventions. Where another document is referenced within this document, an endnote is provided with additional information about that document such as the citation, full formal name or a URL where it can be found. Where another section of the Business Rules is referenced from within the Business Rules, the title is capitalized (for example, when the remedies of section 5.3 are referenced, the term "Recourse" is used). Defined terms are also capitalized when used throughout the document. The definitions of such terms are contained in Appendix 5, the glossary. Defined terms include other parts of speech of the same word when that word has been capitalized in this document (for example, the words "Approved" and "Approve").

It is expected that this document will be used as a "template", meaning it will serve as an initial version that can be amended as the E-Authentication Federation evolves. To achieve clarity and ease of use, only the minimum necessary overlay of legal and contextual verbiage was included. Where possible, other documents containing additional more specific language have been included by reference. In addition, commercial terms and conditions customary in GSA contracts are expected to result from a future solicitation and procurement process in connection with the E-Authentication Federation.

The E-Authentication Federation Business Rules and Participation Agreements were prepared for the General Services Administration and drafted by Daniel J. Greenwood, Esq. with input from Linda Elliott and RJ Schlecht.

**Business Rules**  
**E-Authentication Federation**  
Version 1.0, 2004-NOV-23

**1. Title**

This document shall be known and may be cited as the “E-Authentication Federation Business Rules”, or, as referenced herein, as “Business Rules”.

**2. Scope**

**2.1. Scope of Rules**

Signatories to these Business Rules agree that these Business Rules govern participation in the E-Authentication Federation, administered by the General Services Administration of the U.S. Federal Government (GSA). The GSA, or its authorized agent, shall Certify Credential Services of a Credential Service Provider (CSP). Certified Credentials of a GSA Approved CSP may be accepted, validated and relied upon by GSA Approved Relying Parties. Such acceptance, validation or reliance need not require the use of any additional contract between an Approved CSP and an Approved Relying Party.

**2.2. Agreements and Conduct Outside Scope of Rules**

Nothing in these Rules shall be construed to prevent Approved CSPs and Relying Parties from executing such additional agreements among themselves as they see fit, including agreements covering the use of services, transactions or Credentials, including identity assertions or parts of such assertions. However, nothing in such additional agreement or services, transactions or Credentials covered by such agreement may conflict with any part of the Rules, processes or technologies specified or referenced in these Business Rules. Any activity covered by an addenda to the Participation Agreement, an addenda to these Business Rules or by any other contract or agreement other than the Participation Agreement or these Business Rules, is subject to the terms of that other agreement and is outside the scope of these Business Rules.

**2.3. Rules Appearing in Multiple Documents**

Any provision of these Business Rules that duplicates or emphasizes identical or similar provisions of other normative documents governing the E-Authentication Federation shall not be construed as to lessen the enforceability of any other provisions that have not been duplicated or emphasized.

**3. Participation**

**3.1. Eligibility**

The United States Federal Government or any State or Local government of the United States is eligible to become a CSP or a Relying Party under these Rules, provided it is a legal entity and the other requirements set forth in these Rules are satisfied. In addition, any legal entity, including a non-governmental organization, is eligible to become a CSP under these Rules, provided the other requirements set forth in these Rules are satisfied.

**3.2. Participation Requirements**

**3.2.1. Relying Parties**

Approval by the GSA is necessary for a Relying Party to participate in the EAuthentication Federation. A Relying Party must be a signatory to these Business Rules as a prerequisite to approval by the GSA. A party becomes a signatory Relying Party by executing the Relying Party Participation Agreement with GSA. Each such Relying Party Participation Agreement includes obligations whereby these Business Rules, as periodically amended, are incorporated by reference and consented to.

**3.2.2. CSPs**

Approval by the GSA is necessary for a CSP to participate in the E-Authentication Federation. A CSP must be a signatory to these Business Rules as a prerequisite to approval by the GSA. A party becomes

a signatory CSP by executing the CSP Participation Agreement with GSA. A CSP Participation Agreement may be executed directly with the GSA, or as part of a formal solicitation and procurement process the GSA may require. Each such CSP Participation Agreement includes obligations whereby these Business Rules, as periodically amended, are incorporated by reference and consented to.

A signatory CSP must also have one or more Credential Services Certified according to the applicable requirements of GSA, including the Credential Assessment Framework Suite (CAF)<sup>1</sup>, and be added to the E-Authentication Federation Trusted Credential Service Provider List<sup>2</sup> as a prerequisite for Approval by GSA to participate in the EAuthentication Federation.

### **3.2.3. End-Users**

Any party participating in the E-Authentication Federation as an End-User must have an agreement with an Approved CSP. Such agreement must contain such minimum terms as are required under these Business Rules and the CSP Participation Agreement. End-Users are considered participants in the E-Authentication Federation, but are not direct signatories to these Business Rules.

## **4. Roles and Obligations**

### **4.1. GSA Role and Obligations**

The General Services Administration of the United States Federal Government (GSA) is the party responsible for policy and operations related to the E-Authentication Federation. The GSA is responsible for defining and managing the roles, relationships and mutual obligations among parties operating in the E-Authentication Federation. The GSA uses Business Rules and Participation Agreements as a method of defining these roles, relationships and obligations in a formal and, as needed, enforceable manner. The GSA shall provide processes for determining qualification of any party in the E-Authentication Federation. In the course of such activities, as well as ongoing oversight of participant and system performance, the GSA shall act as coordinator and policy enforcement body for the E-Authentication Federation. The GSA may designate offices, departments or other organizational units within the GSA or otherwise within the United States Federal Government to exercise such rights or obligations defined under these Business Rules.

#### **4.1.1. Operating Authorization**

GSA actions in administering the E-Authentication Federation support the authentication component of the U.S. Federal Enterprise Architecture<sup>3</sup>. The President's Management Agenda of 2001<sup>4</sup> directed GSA to lead the operation of the E-Authentication Federation, which implements OMB- M04-04<sup>5</sup> and NIST SP 800-63<sup>6</sup>.

#### **4.1.2. Promulgation and Amendment of Business Rules and Other Documents**

GSA shall formalize and may amend these Business Rules pursuant to its duty to administer and manage the E-Authentication Federation. Amendments to these Business Rules must comply with the E-Authentication Federation Business Rules Amendment Process<sup>7</sup>. In addition to these Business Rules, the following materials are also formal normative documents defining rights, obligations, processes and other binding statements relative to the E-Authentication Federation: the CSP Participation Agreement, the Relying Party Participation Agreement, the Credential Assessment Framework<sup>8</sup>, the Technical Architecture<sup>9</sup>, the Interface Specification<sup>10</sup> and the Relying Party Requirements Document.

#### **4.1.3. Relying Party and CSP Approval**

The GSA is responsible for determining whether to Approve a Relying Party for participation in the E-Authentication Federation. The GSA shall formalize and may amend periodically requirements for CSP Certification and is responsible for making approval decisions for participation in the E-Authentication Federation by Certified CSPs. The GSA shall formalize, maintain and update as needed a Trusted Credential Service Provider List<sup>11</sup> of Approved and Certified CSPs participating in the E-Authentication Federation. This list shall be a public document and include, at a minimum, the names of each CSP that has been successfully Certified, and the Level of Assurance of each Certified Credential Service of that CSP. The GSA shall determine what continuing audit and other compliance requirements shall satisfy maintenance of Certification and the terms of these Business Rules.

#### **4.1.4. Service Offerings**

To facilitate use of the E-Authentication Federation, the GSA will provide policies, various Architectural Components, business relationship management, Business Rules and Participation Agreements and other offerings.

##### **4.1.4.1. Architectural Components**

GSA may implement and make available to Approved Parties Architectural Components to facilitate use of the E-Authentication Federation, including the EAuthentication Portal identified in the Technical Architecture<sup>12</sup>, Step-Down Translator(s), Schema Translator(s) and Validation Services. The GSA may incorporate additional components.

##### **4.1.4.2. Interoperability Requirements**

The GSA shall operate an interoperability laboratory for the purpose of testing interoperability of products, software, communication specifications and other relevant aspects of current and potential future enhancements to the EAuthentication Federation.

##### **4.1.5. Contact Information**

For current information related to the E-Authentication Federation and these Business Rules, contact the contact E-Authentication Program Director of the General Services Administration of the U.S. Federal Government or see <http://cio.gov/eauthentication/>.

#### **4.2. Relying Party Role and Obligations**

##### **4.2.1. Relying Party Participation Agreement**

A Relying Party is obliged to execute a Relying Party Participation Agreement as a prerequisite to approval for participation in the E-Authentication Federation. The current Relying Party Participation Agreement is included as Appendix 2.

##### **4.2.2. Interface Specification, Approved Software Use and Upgrade**

A Relying Party is obliged to comply with and use the E-Authentication Interface Specification<sup>13</sup> to participate in, communicate through or connect with the EAuthentication Federation. A Relying Party is obliged to use software on the Approved Communications Software<sup>14</sup> list or interface software otherwise approved by GSA. In order to maintain Approval to participate in the Federation, each Relying Party is obliged to follow requirements set by GSA to stay current with Approved Communications Software<sup>15</sup>.

##### **4.2.3. Security and Privacy Compliance**

The following Rules apply to any information system supporting the Agency Application of the Relying Party that is part of the U.S. Federal Government. An Approved Relying Party is obliged to comply with OMB Circular No. A-130<sup>16</sup> including Appendix III to OMB Circular No. A-130<sup>17</sup>, with respect to any information technology system of the Relying Party.

An Approved Relying Party is obliged to comply with the Privacy Act of 1974<sup>18</sup> and OMB Memorandum M-03-22<sup>19</sup>, including where required, performing a Privacy Impact Assessment with respect to the handling of personally identifiable information of an End-User.

An Approved Relying Party that is not part of the U.S. Federal Government must certify to the GSA that it is in compliance with equivalent safeguards and relevant requirements. GSA, in its discretion, shall determine whether such certification is sufficient.

##### **4.2.4. Reasonable Reliance and Level of Assurance**

A Relying Party is obliged to determine for itself whether to rely on the authentication status of an End-User and whether to authorize usage of the Agency Application. In order to determine the authentication status of an End-User, a Relying Party must:

. Determine for itself the level of Agency Application risk, and therefore the needed Level of Assurance, as per the guidance in OMB M-04-04<sup>20</sup> and NIST SP 800-63<sup>21</sup>, using the GSA-provided ERA tool or any other method it deems acceptable;

- . Determine communications or other interactions through the Federation are with Approved CSPs, in accordance with the Approved Party Authentication requirements in Section 4.4.5 of these Rules;
- . Determine that the Level of Assurance of an Approved Credential is not less than the Relying Party required Level of Assurance for its Agency Application; and
- . Determine that the credential is currently valid as per the E-Authentication Technical Architecture<sup>22</sup>, including, as relevant, the Interface Specification<sup>23</sup>.

Communications and other interactions with a CSP or End-User by a Relying Party must comply with the requirements in this Section in order to be within the scope of the EAuthentication Federation and governed by these Business Rules.

### **4.3. CSP Role and Obligations**

#### **4.3.1. CSP Certification**

An Approved CSP is obliged to achieve Certification and be added to the Trusted Credential Service Provider List<sup>24</sup>. Certification is achieved upon successful completion of policy mapping, assessment of the CSP according to the CAFs<sup>25</sup> and operational testing.

#### **4.3.2. CSP Participation Agreement**

A CSP is obliged to execute a CSP Participation Agreement as a prerequisite to approval for participation in the E-Authentication Federation, thereby agreeing to abide by these Business Rules. The current CSP Participation Agreement is included as Appendix 1.

#### **4.3.3. CSP Continuing Audit Requirement**

An Approved CSP is obliged to undergo an audit, no less than annually, confirming compliance with continuing requirements arising out of Certification and with the obligations and other relevant terms of these Business Rules and the CAF<sup>26</sup>. An audit planned or undergone by a CSP unrelated to the E-Authentication Federation may be sufficient to meet this requirement in whole or in part, in the discretion of the GSA.

#### **4.3.4. Material Change to CSP, Credential Services or Credential**

An Approved CSP may be required by the GSA to undergo an additional Certification in whole or in part, to re-Certify one or more Credential Services at the same or different Levels of Assurance or to accept Suspension or Termination of Certification and Participation in the E-Authentication Federation when audit results indicate material changes in the CSP, the Certified Credential Services or in the Credentials it issues or other relevant changes that bring the CSP out of compliance with continuing requirements.

#### **4.3.5. Interface Specification**

A CSP is obliged to comply with and use the E-Authentication Technical Architecture<sup>27</sup> to participate in, communicate through or connect with the E-Authentication Federation.

#### **4.3.6. End-User Notice Terms**

E-Authentication Federation End-User notice terms include agreement to maintain the security of each Approved Credential, including any Token housing each Credential, and to report to the appropriate authorities of the CSP or otherwise any known or reasonably suspected compromise of such Credential or Token.

Every Approved CSP is encouraged to assure the affirmative manifestation of assent by each End-User to E-Authentication Federation notice terms. Every Approved CSP is obliged to assure that each End-User has, at least, been given notice of and the opportunity to review E-Authentication Federation End-User notice terms

### **4.4. General Obligations**

Every Approved Relying Party and Approved CSP (Approved Party) is obliged to comply with the following Rules.

#### **4.4.1. Record Keeping**

Any Approved Party may be requested to transmit to GSA transaction information for the purpose of investigating and correcting interoperability issues that may arise between parties operating in the E-Authentication Federation. In addition, every Approved Party, in order to facilitate GSA resolution of disputes under Section 5 of these Business Rules, is obliged to keep records sufficient to preserve relevant evidence of the facts related to the dispute in question. To the extent that information identified in this Section constitutes Personally Identifiable Information within a System of Records under the Privacy Act of 1974<sup>28</sup>, nothing in this section shall be construed to authorize or permit the communication of such information about an End-User without that End-User's informed consent.

#### **4.4.2. Federation Security and Reliability**

Every Approved Party agrees to coordinate with the GSA in safeguarding the security and reliability of the E-Authentication Federation. GSA may render inaccessible any Architectural Component of the E-Authentication Federation to prevent or cease serious harm to the Federation. Every Approved Party agrees the GSA reserves the right to suspend participation by any Participant in the E-Authentication Federation in accordance with the E-Authentication Federation Participation Suspension Policy<sup>29</sup>, and only under extraordinary circumstances necessary to prevent or cease serious harm to the EAuthentication Federation.

To assure the reliable operation of the E-Authentication Federation, every Approved Party must inform GSA through appropriate channels of any material change in a web site, use of an Architectural Component or other technology or business modification that can reasonably be expected to disrupt, significantly delay or prevent communications through the Federation. This notice must occur in a timely manner prior to the date of any such planned modification.

#### **4.4.3. Federation Interoperability**

To assure the efficacy and operation of the E-Authentication Federation, every Approved Party must demonstrate to the GSA that its interactions and communications through the Federation comply with the E-Authentication Technical Architecture<sup>30</sup> and will interoperate with the architectural components of the Federation. To this end, every Approved Party must conduct tests of its planned Federation interactions and communications in the Interoperability Lab, or through such other process GSA may designate, to demonstrate compliance and interoperability requirements for the Federation have been met.

#### **4.4.4. Operational and Ongoing Requirements**

Every Approved Party is obliged to comply with application, testing, piloting, production and continuing maintenance requirements set forth by the GSA. These ongoing requirements include continued compliance with the provisions of the CAF<sup>31</sup> and with applicable requirements documents defining operational sufficiency for participation in the E-Authentication Federation. Nothing in this section, however, shall be construed to prevent any Approved Party from extending, adding to or otherwise applying other technologies or services in accordance with Section 2.2 of these Rules.

#### **4.4.5. Authentication of Approved Parties**

Communications through the E-Authentication Federation are subject to mandatory authentication by the communicating Approved Parties to prevent participation in the Federation by non-Approved Relying Parties or CSPs. To this end, Approved Parties must implement and comply with the E-Authentication Federation Technical Architecture<sup>32</sup> specifications for authenticating approved parties.

#### **4.4.6. End-User Privacy**

Every Approved Party is obliged to assure that each End-User has provided Informed Consent to the sharing of any personally identifiable information related to the End-User by the Approved Party with any other party operating within the E-Authentication Federation, including any personally identifiable information contained in a certificate or other identity assertion as included in the Interface Specification. Under these Business Rules, no Approved CSP or Approved Relying Party is permitted to share

personally identifiable information about an End-User beyond the information provided for in the Interface Specification.

## **5. Enforcement**

### **5.1. Dispute Resolution**

Every Approved Party agrees to attempt in a timely manner to resolve any dispute arising out of or related to the application of these Business Rules or the Participation Agreement executed by that Approved Party in good faith with the other disputants and parties related to the dispute. Each such dispute, the date and successful or attempted resolutions, including changes in policy, practices or technology implementation, shall be reported to the GSA in a timely manner.

To the extent that information identified in this Section constitutes Personally Identifiable Information within a System of Records under the Privacy Act of 1974<sup>33</sup>, nothing in this section or any sub-section shall be construed to authorize or permit the communication of such information about an End-User without that End-User's informed consent.

In the event parties to a dispute are unable, despite their best good faith efforts, to resolve a dispute among themselves, any party may request GSA investigate the dispute potentially leading to Recourse for the aggrieved party.

### **5.2. GSA Investigation**

GSA shall respond to every request to investigate a dispute in a timely manner. GSA may request additional information from one or more parties to the dispute.

#### **5.2.1. Federation Participant Request for Investigation**

In the event good faith efforts to resolve a dispute are not successful among the disputants and other parties, any Participant in the E-Authentication Federation may request that GSA investigate the matter, propose a resolution and, if necessary arbitrate a resolution of the matter. Each such request must be accompanied by a full report of all the relevant information related to the dispute.

#### **5.2.2. GSA Initiated Investigation**

GSA may initiate an investigation based upon the request of any Participant in the EAuthentication Federation, or may initiate an investigation whenever it deems appropriate based on any information it regards as relevant and credible. Without limitation, such information may include reasonable suspicion that an Approved Party is not in compliance with continuing obligations required under these Business Rules.

### **5.3. Recourse**

Based upon the results of its investigation and in accordance with the E-Authentication Federation Participation Suspension Policy<sup>34</sup>, and only under extraordinary circumstances necessary to prevent or cease serious harm to the E-Authentication Federation, the GSA may suspend participation of any Participant in the E-Authentication Federation or render inaccessible any Architectural Component of the Federation by one or more Participants. If the result of an Investigation indicates that an Approved Party is not in compliance with any requirement included directly or by reference under these Business Rules, GSA may require such additional audit, re-Certification or Certification at different Levels of Assurance, to the extent necessary to prevent or cease serious harm to the Federation.

## **6. General Legal Terms**

### **6.1. Limitation Of Liability**

Recourse against the United States for damage caused by negligence of a government employee is controlled by the Federal Tort Claims Act<sup>35</sup>, 28 USC Section 1346 et seq. A non-governmental Approved CSP operating in accordance with the terms of the CSP Participation Agreement and these Business Rules may assert the government contractor defense to tort claims arising under the CSP Participation Agreement and these Business Rules.

There shall be no Recourse for any claim arising out of or in relation to use of or reliance upon an Approved Credential or the E-Authentication Federation against any Approved Party under any theory of liability, beyond the Recourse available under the Federal Tort Claims Act<sup>36</sup>, unless agreed by contract among the relevant parties.

## **6.2. Governing Law**

These Business Rules and any related materials governing the E-Authentication Federation shall be construed and adjudicated according to the laws of the United States of America.

## **6.3. Order of Precedence**

In the event of a conflict between the terms of various E-Authentication Federation related documents, each such document shall be accorded the following order of priority: the Participation Agreement shall be construed to prevail over conflicting terms of any other E-Authentication Federation document, followed in order of precedence by the terms of these Business Rules, followed by the terms of any normative document listed in Section 4.1.2 of these Rules, followed by the terms of any other policies, agreements or other materials formally promulgated for the purpose of documenting legal terms governing participation in the E-Authentication Federation.

## **6.4. Assignment, Succession and Bankruptcy**

No Approved Party may sell, rent, lease, sublicense, assign, grant a security interest in or otherwise transfer any right and/or obligation contained in these Business Rules or the Participation Agreement executed by that Approved Party, except as permitted herein. Any Approved Party may request of GSA permission for assignment or succession to a different party, including a creditor of the Approved Party, of part or all of the rights and/or obligations contained in these Business Rules or the Participation Agreement executed by that Approved Party.

## **6.5. Severability**

If any provision, set of provisions or part of a provision of these Business Rules is held to be unenforceable or otherwise invalid in whole or in part, the remaining provisions shall remain in full force and effect and shall be construed to the maximum extent practicable as a consistent and reasonable entire agreement.

## **6.6. Counterparts**

These Business Rules may be executed as an agreement simultaneously in one or more counterparts, each of which shall be deemed to be an original, but all of which together shall constitute one and the same instrument.

## **6.7. Waiver**

Neither party's failure to enforce strict performance of any provision of these Business Rules will constitute a waiver of a right to subsequently enforce such a provision. No written waiver shall constitute, or be construed as, a waiver of any other obligation or condition of these Business Rules.

## **6.8. Responsibility For Taxes, Expenses**

Each Approved Party agrees that it is solely responsible for the payment of taxes or expenses incurred by that Approved Party arising out of or related to participation in the EAuthentication Federation.

## **7. Interpretation and Amendment**

The terms of these Business Rules shall be interpreted by the GSA so as to avoid conflict or inconsistencies between the various provisions and between these Business Rules, applicable Participation Agreements and other relevant E-Authentication Federation materials. These Business Rules may be amended according to the E-Authentication Federation Business Rules Amendment Process<sup>37</sup>, however no such amendment shall go into legal effect earlier than 90 days from the time notice is afforded to Approved Relying Parties and Approved CSPs. Notice may be provided of amendment to these Business Rules and other matters related to the operation of the E-Authentication Federation by electronic mail to the contact person(s) indicated for each

Approved Party and by posting to the E-Authentication Federation web site.

**Appendix 1**  
**E-Authentication Federation**  
**CSP Participation Agreement**

Version 1.0, 2004-NOV-23

Drafted by [Daniel Greenwood](#), Esq.

[personal email and telephone redacted in public draft and replaced by URL]

<http://www.civics.com>

**1. Recitals**

This Participation Agreement constitutes the legal basis for an organization to become a Credential Service Provider (CSP) within the E-Authentication Federation.

**2. Parties**

The parties to this Participation Agreement are the General Services Administration of the United States federal government (GSA) and \_\_\_\_\_ (CSP).

**3. Agreement to Abide by Business Rules**

By signing this Participation Agreement, the CSP agrees to abide by the E-Authentication Federation Business Rules, as in effect during the period of CSP participation in the EAuthentication Federation, and which are expressly incorporated into and make a part of this Agreement.

**4. Dispute Resolution: Notice, Investigation, Resolution and Recourse**

CSP agrees that the E-Authentication Business Rules Dispute Resolution and Recourse provisions cover issues between Approved CSPs and Relying Parties operating in the Federation. Any dispute resolution process and rules between the CSP and an End-User must be defined and pursued between the CSP and the End-User, and such terms are not within the scope of the Business Rules of this Participation Agreement.

**5. Termination and Suspension**

The terms of this Participation Agreement and the Business Rules cease to apply to any CSP as of the effective date of termination of Participation in the E-Authentication Federation.

**5.1. Voluntary**

Participation in the E-Authentication Federation may be terminated by CSP through written notice to GSA, to avoid the imminent effect of amended language to the Business Rules. Such notice shall be effective no less than 30 calendar days from the date of receipt by GSA. Participation in the E-Authentication Federation may be terminated by mutual agreement between the GSA and CSP.

**5.2. Involuntary**

GSA may suspend the participation of CSP in the E-Authentication Federation, in accordance with the E-Authentication Federation Participation Suspension Policy<sup>38</sup>, under extraordinary circumstances necessary to prevent or cease serious harm to the E-Authentication Federation. GSA may terminate the participation of CSP in the E-Authentication Federation in writing for cause, including breach by the CSP of the terms of this Participation Agreement or the Business Rules.

**6. Confidentiality and Non-Disclosure**

GSA agrees to execute any reasonable confidentiality and/or non-disclosure agreements with the CSP that may be required as a condition of accepting credentials of that CSP and according to the Business Rules. GSA further agrees to require consent to the relevant terms of such agreements by any Relying Party to whom the terms may apply.

## **7. Legal Terms**

### **7.1. Limitation Of Liability**

Recourse against the United States for damage caused by negligence of a government employee is controlled by the Federal Tort Claims Act<sup>39</sup>, 28 USC Section 1346 et seq. A non-governmental Approved CSP operating in accordance with the terms of this CSP Participation Agreement and the E-Authentication Federation Business Rules may assert the Government Contractor Defense to tort claims arising under this CSP Participation Agreement and the E-Authentication Federation Business Rules.

There shall be no Recourse for any claim arising out of or in relation to use of or reliance upon an Approved Credential or the E-Authentication Federation against any Approved Party under any theory of liability, beyond the Recourse available under the Federal Tort Claims Act<sup>40</sup>, unless agreed by contract among the relevant parties.

### **7.2. Governing Law**

This CSP Participation Agreement and any related materials governing the E-Authentication Federation shall be construed and adjudicated according to the laws of the United States of America.

### **7.3. Integration and Order of Precedence**

This CSP Participation Agreement and the E-Authentication Federation Business Rules constitute the entire agreement of the parties with respect to participation in the EAuthentication Federation. In the event of a conflict between the terms of various EAuthentication Federation related documents, documents shall be accorded the following order of priority: This CSP Participation Agreement shall be construed to prevail over the terms of any other document, followed in order of precedence by the terms of the EAuthentication Federation Business Rules, followed by the terms of any other policies, agreements or other materials formally promulgated for the purpose of documenting legal terms governing participation in the E-Authentication Federation.

### **7.4. Assignment, Succession and Bankruptcy**

CSP agree it may not sell, rent, lease, sublicense, assign, grant a security interest in or otherwise transfer any right and/or obligation contained in this CSP Participation Agreement or the E-Authentication Federation Business Rules except as permitted herein. CSP may request of GSA permission for assignment or succession to a different party, including a creditor of the CSP, of part or all of the rights and/or obligations contained in this CSP Participation Agreement or the E-Authentication Federation Business Rules. Any prohibited assignment shall be null and void.

### **7.5. Severability**

If any provision, set of provisions or part of a provision of this CSP Participation Agreement is held to be unenforceable or otherwise invalid in whole or in part, the remaining provisions shall remain in full force and effect and shall be construed to the maximum extent practicable as a consistent and reasonable entire agreement.

### **7.6. Responsibility For Taxes, Expenses**

CSP agrees that it is solely responsible for the payment of taxes or expenses incurred by the CSP arising out of or related to participation in the E-Authentication Federation.

## **8. Amendment**

This Participation Agreement may be amended by agreement of the parties, reflected by a signed writing.

## **9. Signatures**

\_\_\_\_\_  
CSP

\_\_\_\_\_  
GSA

**Appendix 2**  
**E-Authentication Federation**  
**Relying Party Participation Agreement**

Version 1.0, 2004-NOV-23

Drafted by [Daniel Greenwood](#), Esq.

[personal email and telephone redacted in public draft and replaced by URL]  
<http://www.civics.com>

**1. Recitals**

This Relying Party Participation Agreement constitutes the legal basis for an organization to become a Relying Party within the E-Authentication Federation.

**2. Parties**

The parties to this Participation Agreement are the General Services Administration of the United States federal government (GSA) and \_\_\_\_\_ (Relying Party).

**3. Agreement to Abide by Business Rules**

By signing this Participation Agreement, the Relying Party agrees to abide by the EAuthentication Federation Business Rules, as in effect during the period of participation in the EAuthentication Federation, and which are expressly incorporated into and make a part of this Agreement.

**4. Compliance With Requirements**

Relying Party agrees that satisfactory completion of the GSA Relying Party Requirements Document, including confirmation of required privacy, regulatory compliance and technical practices, is a pre-requisite to participation in the E-Authentication Federation and must be finalized approval for inclusion in the E-Authentication Federation. Relying Party agrees to maintain continuing compliance with the requirements and other terms contained in the EAuthentication Federation Business Rules, including compliance with the technical, policy and procedural documents incorporated by reference in the E-Authentication Federation Business Rules.

**5. Dispute Resolution: Notice, Investigation and Resolution**

Relying Party agrees that the E-Authentication Business Rules Dispute Resolution and Recourse provisions cover issues between Approved CSPs and Relying Parties operating in the Federation. Any dispute resolution process and rules between the Relying Party and an End-User must be defined and pursued between the Relying Party and the End-User, and such terms are not within the scope of the Business Rules of this Participation Agreement.

**6. Termination and Suspension**

The terms of this Participation Agreement and the Business Rules cease to apply to any Relying Party as of the effective date of termination of Participation in the E-Authentication Federation.

**6.1. Voluntary**

Participation in the E-Authentication Federation may be terminated by written notice to GSA, to be effective no less than 30 calendar days from the date of receipt by GSA. Participation in the E-Authentication Federation may be terminated by mutual agreement between the GSA and Relying Party.

**6.2. Involuntary**

GSA may suspend the participation of any Relying Party in the E-Authentication Federation in accordance with the E-Authentication Federation Participation Suspension Policy<sup>41</sup>, and only under extraordinary circumstances necessary to prevent or cease serious harm to the EAuthentication Federation.

**7. Confidentiality and Non-Disclosure**

Relying Party agrees to execute any reasonable confidentiality and/or non-disclosure agreements participating CSPs may require as a condition of accepting credentials of that CSP and according to the Business Rules.

**8. Liability**

There shall be no Recourse for any claim arising out of or in relation to use of or reliance upon an Approved Credential or the E-Authentication Federation against any Approved Party under any theory of liability, beyond the Recourse available under the Federal Tort Claims Act<sup>42</sup>, unless agreed by contract among the relevant parties.

**9. Amendment**

This Participation Agreement may be amended by agreement of the parties, by a signed, writing.

**10. Signatures**

\_\_\_\_\_  
*Relying Party*  
14

\_\_\_\_\_  
GSA

## **Appendix 3**

### **E-Authentication Federation Business Rules Amendment Process**

Version 1.0, 2004-NOV-23

The E-Authentication Federation Business Rules may be amended according to the following process. Any Approved CSP or Relying Party may certify a request for consideration of a proposed Amendment of the Business Rules to the GSA, including the reasons therefor and proposed amended language. Any such proposed Amendment shall trigger the Consultative Amendment Process, defined below. The GSA may also propose an Amendment triggering the Consultative Amendment Process.

#### **Consultative Amendment Process**

Notice of a proposed Amendment requested by an Approved Party, no later than 30 days from the time the request is received by the GSA, shall be communicated to each Approved Party in the E-Authentication Federation for consideration and comment. Said notice shall be delivered by e-mail to the named contact person(s) in the Participation Agreements of the Approved Parties and may also be posted to the official E-Authentication Federation web site. A period of not less than 30 days shall be afforded Approved Parties to consider, comment upon and, at their discretion, indicate agreement with, disagreement with and/or alternative proposed language to the GSA. The GSA may hold one or more consultative meetings of interested Approved Parties to discuss any proposal and may extend the period for consideration and comment, as needed to accommodate the needs of the parties.

#### **Disposition of Amendment Proposal**

No more than 10 days after the period for consideration and comment has closed, the GSA shall communicate to each Approved Party notice of the disposition of the proposal, including whether the proposal has been rejected and no Amendment will be pursued, or the proposal has been modified, or the proposal has been accepted. Said notice shall be delivered by e-mail to the named contact person(s) in the Participation Agreements of the Approved Parties and may also be posted to the official E-Authentication Federation web site. If the proposal is modified, the modified proposal shall trigger a new Consultative Process, defined above. If the proposal is accepted, it shall trigger the Amendment Incorporation Process defined below.

#### **Amendment Incorporation Process**

An Amendment that has been accepted after a Consultative Amendment Process according to the notice provisions specified in the Disposition of Amendment Proposal process shall go into legal effect no less than 90 days from the date notice has been sent, or such later time as specified in the notice. Any Approved Party may terminate participation in the E-Authentication Federation no less than 30 days from the time of sending notice of termination to the GSA according to the Business Rules, and in every case reserves the right to terminate participation prior to any Amendment coming into full force and effect.

## Appendix 4

### General Overview

Version 1.0, 2004-NOV-23

The E-Authentication Federation is designed to allow electronic access to government services by examining electronic credentials to verify the End-User's identity. This Federation is run by the General Services Administration of the U.S. Federal Government under the name of the EAuthentication Initiative. The E-Authentication Initiative is one of twenty-four Electronic Government (E-Gov) services from the President's Management Agenda, which is intended to improve interfaces between citizens, businesses, and all levels of government.

The credentials may be issued by government agencies, but may also be issued by commercial entities for this purpose or for other purposes. In those cases, the E-Authentication Federation would be providing for reliance on commercially-issued, re-usable credentials. The EAuthentication Federation, including public and private organizations, uses such credentials along with a common technical, policy and legal infrastructure. These Business Rules, and the related Participation Agreements form the cornerstone of the legal aspect of the infrastructure. The Federal Government, in order to support the electronic government initiatives, is undertaking the E-Authentication initiative to allow for federation of identity and creating federation for the government and other entities so that citizens can authenticate to the government. The EAuthentication Federation requires policy and technology infrastructure as well as business rules and participation agreements. The technology infrastructure includes Architectural Components such as a validation service, a discovery portal, a step-down translator and a protocol translator. These components make it possible for parties using different technologies to federate identities from one organization to another. The E-Authentication Federation is the authentication component of the federal enterprise architecture.

The E-Authentication Federation has these key participants: Credential Service Providers (CSPs), End-Users, Relying Parties who are operating Agency Applications (RPs), and the General Services Administration of the U. S. Government, who acts as the administrative, operational, and policy arm of the E-Authentication Federation. End-Users, who will use credentials to access Agency Applications may be government employees or contractors or private citizens who are affiliated with one or more CSPs. That affiliation could include a customer, employee or partnership relationship. Relying Parties may include government agencies at the Federal, State, or local levels.

Credential Service Providers issue credentials to End-Users, who in turn use those credentials to get access to Government services over the world wide web. The E-Authentication Initiative facilitates this process through its service model, which includes policy services, technology services, and customer service.

The E-Authentication Federation utilizes industry standard technologies, implemented through Commercial Off the Shelf Products (COTS). Use of Approved COTS Software is required of all Approved CSPs, Relying Parties and for all communications occurring through the EAuthentication Federation. A complete explanation of the technical architecture is available in the publication 'Technical Approach for the Authentication Service Component'. The architecture supports the concept of credentials at each of four Assurance Levels, allowing the Relying Party to match their acceptance of credentials to the Risk Assessment they will have completed for their Agency Application. Risk assessment guidance is contained in OMB M-04-04<sup>43</sup>. Guidance for credentials at each of the four assurance levels is contained in NIST SP 800-63<sup>44</sup>.

The E-Authentication Federation uses the Security Assertion Markup Language (SAML) and also PKI as enabling technologies allowing for federation of credentials across organizations in both the public and private sectors. Any CSP in the private or public sector issuing credentials that comply with the SAML standard when configured in accordance with the GSA issued Interface Specification can be considered for Approval by GSA to participate in the E-Authentication Federation at Assurance Levels 1 and 2. In

addition, the CSPs operating within the Federal Public Key Infrastructure, PKI Bridge, and issuing credentials under the ACES, FICC, and FPKIPA programs can also be considered for participation at any Assurance Level. Any CSP, whether a provider of SAML or PKI based credentials, must execute a Participation Agreement legally binding it to the E-Authentication Business Rules in order to be Approved for participation. Other technical standards and specifications may be accepted for use within the E-Authentication Federation as they become available at the sole discretion of the GSA.

Both CSPs and RPs will need to meet a number of requirements for participation in the EAuthentication Federation. Guidance on these requirements is contained in documents published by the GSA including E-Authentication Handbook for Federal Government Agencies, EAuthentication Handbook for Credential Service Providers, and the E-Authentication Cookbook. The GSA evaluates the qualifications of potential participants, assists them in matriculating through the qualification, testing, and activation process, and maintains oversight of the EAuthentication Federation operation. In addition, the GSA operates a conformance testing service for COTS products, an interoperability testing service, and runs some technical services that are designed to lessen the technical burden on the participants.

These Business Rules are intended to define the legal terms and overall structure, including roles and obligations governing participation in the E-Authentication Federation. CSPs and Relying Parties sign Participation Agreements which obligate them to the terms of these rules as well as the policies of the GSA. End-Users, while considered participants, do not sign Participation Agreements directly with GSA. Rather, End-Users sign agreements containing approved E-Authentication Federation terms with the CSP who has issued and Approved Credential to that user. Details of operational processes are contained in GSA documents, including the ones referenced above, and many more that are relevant to various aspects of EAuthentication Federation participation, such as interoperability testing. Documents are available through the E-Authentication Federation website at <http://www.cio.gov/eauthentication/>

The following diagram illustrates the organizations which oversee the E-Authentication Federation within the US Government, and the major areas of responsibility for both policy (within the Office of Government-wide Policy) and operations (within the Project Management Office or PMO) for the E-Authentication Federation.

### **Federal E-Authentication Initiative Overview**

In 2001, President Bush initiated several government reform efforts, collectively known as the President's Management Agenda (PMA). The five government-wide efforts focus on Strategic Management of Human Capital, Competitive Sourcing, Improved Financial Performance, Expanded Electronic Government, and Budget and Performance Integration. The Chief Information Officers (CIOs) of the federal agencies have a major role in the achievement of the PMA goals. They lead the implementation of many of the programs that help expand electronic government and provide support to others.

CIO Council contributed to several government-wide initiatives, focusing on reducing costs and improving services to citizens. To facilitate efforts to transform the Federal Government the Office of Management and Budget (OMB) is developing the Federal Enterprise Architecture (FEA), a business-based framework for Government-wide improvement.

Operating under the authority of the OMB, the General Services Administration (GSA) is responsible for the Federal government's electronic authentication effort. Whether through electronic authentication evolution or historical events the Federal Enterprise Architecture is a combination of pre-PMA and new efforts. The Federal government established several significant efforts related to electronic authentication, prior to creation of the Electronic Authentication Initiative. These efforts include Federal Public Key Infrastructure (FPKI), Access Certificates for Electronic Services (ACES), Federal Identity Credentialing Committee (FICC). The E-Authentication Initiative (EAI) provides for incorporation of these prior efforts into the e-Authentication Federation...

## Federal e-Authentication Diagram

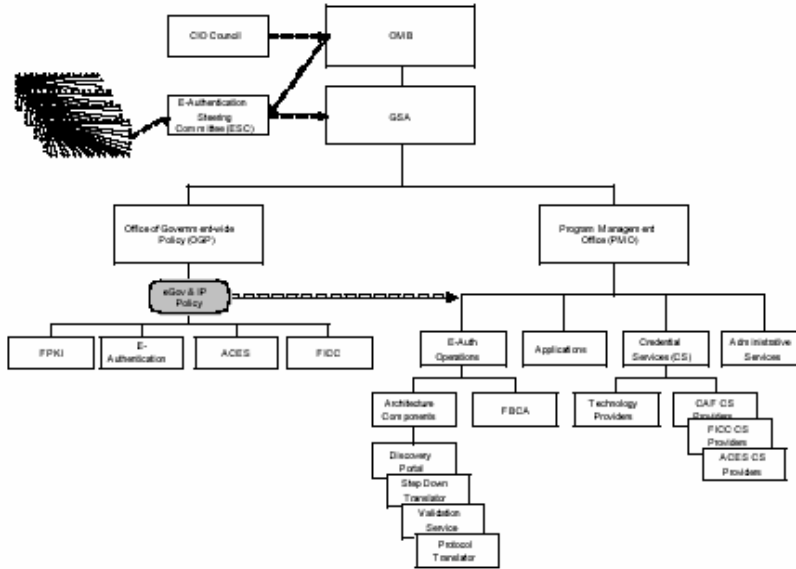


Diagram 1

The Federal authentication architecture is basically divided into two functional areas, policy and operations. Within both policy and operations there are various initiatives to meet the diverse demands of the government. These include historical agency authentication services, various levels of identity assurance, private sector COTS, technical interoperability, and compliance. Please note that this overview uses terms that are not defined and does not use every defined term according to its formal definition. Rather, the document was written for readability and to provide an informal basis to generally understand the overall initiative at a glance.

## Appendix 5

### E-Authentication Business Rules Glossary

Version 1.0, 2004-NOV-23

#### **Agency Application**

A computer applications of a Relying Party that is uniquely identifiable when used within the E-Authentication Federation.

#### **Approved**

Authorization or other acceptance by the GSA for purposes of participation or other inclusion or use in the E-Authentication Federation.

#### **Approved Credential**

A Credential issued by a Certified Credential Service of an Approved Credential Service Provider to an End-User.

#### **Approved Credential Service Provider (Approved CSP)**

A Credential Service Provider that has been approved by the GSA to participate in the EAuthentication Federation.

#### **Approved Parties**

Any Approved Relying Party and Approved Credential Service Provider.

#### **Approved Relying Party**

A Relying Party that has been approved by the GSA to participate in the E-Authentication Federation.

#### **Certified Credential Service**

A Credential Service judged to meet the requirements identified in the Credential Assessment Framework Suite.

#### **Credential**

Digital information used in authentication and access control that bind an identity or an attribute to an End-User's Token or some other property such as his or her current network address. Note that this glossary distinguishes between Credentials, and Tokens while other documents may use the terms interchangeably.

#### **Credential Service**

A service of a Credential Service Provider that provides credentials to subscribers for use in electronic transactions. If a Credential Service Provider offers more than one type of credential then each one is considered a separate Credential Service.

#### **Credential Service Provider**

An organization that offers one or more Certified Credential Services, also known in this document as a CSP.

#### **End-User**

An individual person that has been issued an Approved Credential by an Approved Credential Service Provider and who communicates through the E-Authentication Federation with an Approved Relying Party and whose identity is verifiable with reference to that Credential.

#### **Informed Consent**

Consent voluntarily signified by an End-User who is competent and who understands the terms of the consent and who has been provided in a clear statement with the appropriate knowledge needed to freely

decide without the intervention of any element of force, fraud, deceit, duress, over-reaching or other ulterior form of constraint or coercion.

**Levels of Assurance**

Four level of authentication defined based upon consequences of a false positive authentication or misuse of a Credential. These levels are documented in OMB Memorandum M-04-04.

**Participant**

Any Approved Relying Party, Approved Credential Service Provider or End-User.

**Relying Party**

A party that relies upon a Credential issued by a Credential Service Provider.

**Relying Party Requirements Document**

This document contains the checklist of items necessary for a Relying Party to be approved by GSA for participation in the E-Authentication Federation.

**Rule**

A provision or term of the E-Authentication Business Rules.

**Security Assertion Markup Language (SAML)**

The XML Schema specified by the open standards organization OASIS-OPEN defining a standard framework for creating and exchanging security information between online partners. The specification, and other information provided by the authoring technical committee, may be found at: [http://www.oasisopen.org/committees/workgroup.php?wg\\_abbrev=security](http://www.oasisopen.org/committees/workgroup.php?wg_abbrev=security).

**Technology Architecture Components**

Inclusive of the portal defined in the E-Authentication Federation Technology Architecture, the step-down translator, validation services and the protocol translator.

**Token**

Something that the End-User possesses or knows (typically a key or password) that can be used to remotely authenticate the claimant's identity. Technically, the Token includes a userid and password that ensures Token uniqueness within a Credential domain.

## Appendix 6

### E-Authentication Business Rules Endnotes

Version 1.0, 2004-NOV-23

<sup>1</sup> **Credential Assessment Framework Suite (CAF)**

The GSA published documents defining a process for the Certification of Credential Services of Credential Service Providers, including the Interim PKI Credential Assessment Profile, Interim Password Credential Assessment Profile, Interim PIN Credential Assessment Profile, Interim Credential Assessment Framework, Interim Credential Assessment Guidance and Interim Common Credential Assessment Profile. This suite of documents collectively can be found at <http://cio.gov/eauthentication/CredSuite.htm>.

<sup>2</sup> **E-Authentication Federation Trusted Credential Service Provider List**

The list of Certified Credential Services and their associated Levels of Assurance. This list is published at <http://cio.gov/eauthentication/TCSPlist.htm>.

<sup>3</sup> **U.S. Federal Enterprise Architecture**

A business and performance-based framework to support cross-agency collaboration, transformation, and government-wide improvement, including reference models for business, service components, data, and a technical reference model. Information about this architecture, and the architecture itself, can be found at: <http://www.feapmo.gov/>.

<sup>4</sup> **President's Management Agenda**

A collection of government reform efforts initiated in 2001 including strategic management of human capital, competitive sourcing, improved financial performance, expanded electronic government and budget and performance integration. Information about these initiatives can be found at: [http://www.cio.gov/documents/CIO\\_Council\\_Strategic\\_Plan\\_FY04.pdf](http://www.cio.gov/documents/CIO_Council_Strategic_Plan_FY04.pdf).

<sup>5</sup> **OMB Memorandum M-04-04**

This document is published by OMB regarding e-authentication guidance for federal Agencies. This document can be found at: <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>.

<sup>6</sup> **NIST SP 800-63**

This document is published by the National Institute of Standards and Technology entitled Electronic Authentication Guideline. This document can be found at: [http://cio.gov/eauthentication/documents/SP800-63V6\\_3\\_3.pdf](http://cio.gov/eauthentication/documents/SP800-63V6_3_3.pdf).

<sup>7</sup> **E-Authentication Federation Business Rules Amendment Process**

Definition of the circumstances and procedures necessary to formally amend the EAuthentication Federation Business Rules. This document can be found in Appendix 3 of the Business Rules.

<sup>8</sup> See note 1.

<sup>9</sup> **E-Authentication Federation Technical Architecture**

Suite of documents defining required implementations and configurations of technology for use in the E-Authentication Federation, including the Interface Specification relevant to use of SAML and path discovery and validation requirements relevant to PKI. This suite of documents can be found at: <http://cio.gov/eauthentication/TechSuite.htm>.

<sup>10</sup> **Interface Specification**

Interface specifications for the SAML Artifact Profile for use in the E-Authentication Federation. This document can be found at: <http://cio.gov/eauthentication/documents/SAMLspec.pdf>.

<sup>11</sup> See note 2.

<sup>12</sup> See note 9.

<sup>13</sup> See note 10.

<sup>14</sup> **Approved Communication Software**

Software approved by the GSA for communications through the E-Authentication Federation. The list of such software, along with the technology providers of those

products, can be found at:

<http://www.cio.gov/eauthentication/documents/ApprovedProviders.htm>

<sup>15</sup> See note 14.

<sup>16</sup> **OMB Circular No. A-130**

This document is published by OMB regarding the management of federal information resources. This document can be found at:

<http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html>.

<sup>17</sup> **OMB Circular No. A-130, Appendix III**

This document is published by OMB regarding security of federal automated information resources. This document can be found at:

[http://www.whitehouse.gov/omb/circulars/a130/a130appendix\\_iii.html](http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html).

<sup>18</sup> **Privacy Act of 1974**

Federal legislation defining allowed federal collection, use or dissemination of personal information. This legislation may be cited as 5 USC § 552a, and can be found at:

[http://www.law.cornell.edu/uscode/html/uscode05/usc\\_sec\\_05\\_00000552---a000-.html](http://www.law.cornell.edu/uscode/html/uscode05/usc_sec_05_00000552---a000-.html).

<sup>19</sup> **OMB Memorandum M-03-22**

This document is published by OMB regarding guidance for implementing the privacy provisions of the e-government act of 2002. This document can be found at:

<http://www.whitehouse.gov/omb/memoranda/m03-22.html>.

<sup>20</sup> See note 5.

<sup>21</sup> See note 6.

<sup>22</sup> See note 9.

<sup>23</sup> See note 10.

<sup>24</sup> See note 2.

<sup>25</sup> See note 1.

<sup>26</sup> See note 1.

<sup>27</sup> See note 9.

<sup>28</sup> See note 18.

<sup>29</sup> **E-Authentication Federation Participation Suspension Policy**

A policy defining the extraordinary circumstances under which an Approved Party may have participation in the Federation suspended. As of the date of publication of version 1 of the E-Authentication Business Rules, this document is not yet finalized.

<sup>30</sup> See note 9.

<sup>31</sup> See note 1.

<sup>32</sup> See note 9.

<sup>33</sup> See note 18.

<sup>34</sup> See note 29.

<sup>35</sup> **Federal Tort Claims Act**

Federal legislation defining U.S. Federal Government liability under tort law. This legislation may be cited as 28 USC § 1346 et seq. and can be found at:

[http://www.law.cornell.edu/uscode/html/uscode28/usc\\_sup\\_01\\_28\\_10\\_VI\\_20\\_171.html](http://www.law.cornell.edu/uscode/html/uscode28/usc_sup_01_28_10_VI_20_171.html).

<sup>36</sup> See note 35.

<sup>37</sup> See note 7.

<sup>38</sup> See note 29.

<sup>39</sup> See note 35.

<sup>40</sup> See note 35.

<sup>41</sup> See note 29.

<sup>42</sup> See note 35.

<sup>43</sup> See note 5.

<sup>44</sup> See note 6.