

Smart Portal

Version 1.0

May 2, 2014

**Proprietary and Confidential**

**For Authorized Use Only**

Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Description | Version | Author |
| 05/02/2014 | Document Publication | 1.0 | Kossi Azoumaro |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1. INFORMATION SYSTEM NAME/TITLE 5](#_Toc384808707)

[2. EAUTHENTICATION LEVEL DEFINITIONS 5](#_Toc384808708)

[3. HOW TO SELECT YOUR EAUTHENTICATION LEVEL 6](#_Toc384808709)

[4. EAUTHENTICATION LEVEL SELECTION 6](#_Toc384808710)

List of Tables

[Table 1-1. Information System Name and Title 5](#_Toc384808713)

[Table 3-1. Potential Impacts for Assurance Levels 6](#_Toc384808714)

[Table 4-1. EAuthentication Level 6](#_Toc384808715)

1. INFORMATION SYSTEM NAME/TITLE

This EAuthentication Plan provides an overview of the authentication level for the Smart Portal in accordance with OMB Memo M-04-04.

Table 1-1. Information System Name and Title

|  |  |  |
| --- | --- | --- |
| Unique Identifier | Information System Name | Information System Abbreviation |
| SP12345 | Smart Portal | SMP |

1. EAUTHENTICATION LEVEL DEFINITIONS

*OMB Memo M-04-04, EAuthentication Guidance for Federal Agencies* requires that federal information system owners determine the system’s electronic authentication (EAuthentication) requirements to minimize the potential impact of authentication errors and misuse of credentials. The OMB memo defines four authentication levels to categorize a federal information system’s EAuthentication posture. The OMB Memo defines four EAuthentication levels as:

* Level 1: Little or no confidence in the asserted identity’s validity
* Level 2: Some confidence in the asserted identity’s validity
* Level 3: High confidence in the asserted identity’s validity
* Level 4: Very high confidence in the asserted identity’s validity

**Note:** OMB Memo M-04-04 can be found at the following URL: <http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf>

The objective for selecting the appropriate EAuthentication level for the candidate system is so that the system owner can then more easily proceed to select the right technology solution to implement the designated level. Guidance on selecting the system authentication technology solution is available in *NIST SP 800-63, Revision 1, Electronic Authentication Guidance*.

**Note:** NIST SP 800-63, Revision 1 can be found at the following URL: <http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf>

1. HOW TO SELECT YOUR EAUTHENTICATION LEVEL

Determine what the qualitative risk exposure would be to the authentication transaction process regardless of the technology used. Select the lowest level that will cover all potential impact identified according the Table 3-1.

Table 3-1. Potential Impacts for Assurance Levels

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Assurance Level Impact Profile | | | |
| Potential Impact Categories for Authentication Errors | 1 | 2 | 3 | 4 |
| Inconvenience, distress or damage to standing or reputation | Low | Mod | Mod | High |
| Financial loss or agency liability | Low | Mod | Mod | High |
| Harm to agency programs or public interests | N/A | Low | Mod | High |
| Unauthorized release of sensitive information | N/A | Low | Mod | High |
| Personal Safety | N/A | N/A | Low | Mod, High |
| Civil or criminal violations | N/A | Low | Mod | High |

1. EAUTHENTICATION LEVEL SELECTION

*Instruction: Please use OMB Memo M-04-04 and NIST SP 800-63, Revision 1 to assist you in selecting an EAuthentication Level for the candidate system. Please note that FedRAMP does not currently perform assessments for systems categorized as High sensitivity.*

The Smart Think has identified that they support the EAuthentication Level that has been selected for the Smart Portalas noted in Table 4-1. The selected EAuthentication Level indicated below is supported for federal agency consumers of the cloud service offering. Implementation details of the EAuthentication mechanisms are provided in the System Security Plan under control IA-2.

Table 4-1. EAuthentication Level

|  |  |  |
| --- | --- | --- |
| EAuthentication Level | Maximum Impact Profile | Selection |
| Level 1: no identity proofing requirement | Low |  |
| Level 2: single factor remote authentication | Low |  |
| Level 3: multi-factor remote authentication | Moderate |  |
| Level 4: multi-factor remote authentication; hard crypto tokens | High |  |

[This page left intentionally blank.]