1

2

3

4 **Identity Assurance Framework:**

5 **US Federal Privacy Profile**

6

7

8 **Version: 1.0**

9 **Date:** 2010-06-24

10 **Editor:** David Wasley, Internet 2

11 Joni Brennan, Kantara Initiative

12 **Contributors:**

13 <http://kantarainitiative.org/confluence/x/7gKDAg>

14

15 **Status:** This document is a **Kantara Initiative Report**, approved by the Identity

16 Assurance WG (see section 3.9 and 4 of the Kantara Initiative Operating Procedures)

17 **Abstract:**

18 Kantara Initiative Federal Privacy Profile for CSPs that desire certification under the

19 IAF for interoperation with US Federal Agency applications under the Open

20 Government program.

21

22 **Filename:** kantara-report-iawg-iaf-us-federal-privacy-profile-1.0

23

24

**Kantara Initiative Final Report** [**www.kantarainitiative.org**](http://www.kantarainitiative.org/)

1

25 **Notice:**

26 This document has been prepared by Participant s of Kantara Initiati ve. Per mi ssi on i s

27 hereby granted to use the document solel y for t he purpose of i mplementi ng t he

28 Specification. No ri ght s are granted to prepare derivative work s of thi s S pecification.

29 Entities seeking per mi ssi on to r eproduce portions of thi s document for other uses mu st

30 contact Kantara I nitiati ve to deter mi ne whether an appropriate license for such use i s

31 availabl e.

32

33 Implementation or use of certai n element s of t hi s document may require licenses under

34 third party i nt ellectual property ri ght s, includi ng wit hout li mitation, patent ri ghts. The

35 Participant s of and any other contributor s to the Specification are not and shall not be held

36 responsible in any manner for identifyi ng or faili ng to identify any or all such t hird party

37 intellectual property right s. Thi s Specification i s provi ded "AS IS," and no Participant in

38 the Kantara I nitiative makes any warrant y of any kind, expressed or implied, includi ng any

39 i mplied warranties of merchantability, non -infringement of t hir d party i ntellectual property

40 right s, and fit ness for a particular purpose. I mplementer s of thi s Specifi cation are advi sed

41 to review t he Kantara Initiative’ s website ([http://www.kantar ainitiative.org)](http://www.kantarainitiative.org/) for

42 information concer ni ng any Necessary Claims Disclosure Notices t hat have been received

43 by t he Kantara Initiati ve Board of Tru st ees.

44

45 The content of t hi s docu ment i s copyright of Kantara Initiati ve. © 2010 Kantara Initiati ve.

46

47 **1 INTRODUCTION**

48 **Kantara Initiative Federal Privacy Profile for CSPs that desire certification under**

49 **the IAF for interoperation with US Federal Agency applications under the Open**

50 **Government program.**

51

52 This profile is required for use with US Federal gover nment applications in conjunction

53 with Kantara I nitiative certified CSP s. Thi s supplement s t he Kantara IAF level of

54 assurance requirement s found in the S AC. No requirement s found in t he IAF SAC or t hi s

55 Profile appl y directly to Rel yi ng Party Appli cati ons (RP s). The Kantara I nitiative

56 Identity Assurance Program, acting in t he capacity of a Trust Framework Provider to t he

57 US Federal Gover nment, assu mes t hat all US Agency RP applications will operate in

58 compliance to all US Federal pri vacy and identit y management policies, laws and

59 regulations.

60 The Credential Service Provider (CSP) must assert and comply with an Identity Subj ect

61 Privacy Policy t hat provides for at least t he foll owi ng:

62

63 a. **Informed Consent** – At t he ti me t he Identity Subject i nitiates regi stration, the CSP

64 must provi de t he Subj ect a general description of the ser vice and how it operat es

65 includi ng what i nfor mation, if any, may be released by default to a ny Rel yi ng Party

66 and, i f t he Subj ect indi cates i nt ent to use the ser vice to gai n access to Federal

67 gover nment applications, must make available to the Identity Subject what additional

68 information, if any, may be released to such applications. The Subj ect must indicate

69 consent to these provi sions before regi stration can be completed.

70

71 CSPs should provide a mechani sm for Identit y Subject s to deny release of

72 indi vidual attributes to Federal gover nment applications, as specified and

73 specifically acco mmodat ed for in the ICAM approved Aut henti cation Scheme

74 being utilized by the CSP. It is recognized, and t he Identity Subj ect should be

75 cautioned t hat such denial may result in a denial of servi ce by t he application

76 unless alter nate means of access are provided to the Identity Subject by t he

77 application it sel f.

78

79 Note: CSPs are not expect ed to provide such a mechanism for attribute -level

80 opt- out for I dentit y Subject s when t he Identit y Subject is engaging wit h a

81 gover nment application on behal f of t heir employer or uni ver sit y and such

82 attributes ar e required by t he RP application to complete the transaction, pre-

83 arranged by policy agreed t o between t he CSP and t he RP well in advance of

84 the transaction.

85

86 b. **Optional Participation –** Identity Subject s t hat are member s, for example

87 employees, facult y, or student s, of an or ganization t hat provides identity ser vi ces as

88 part of it s business processes should be allowed to opt -out of usi ng t hat

89

90

91

92

93

94

95

96

97

98

99

100

101

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

120

121

122

123

124

125

126

127

128

129

130

131

organi zation’ s identit y ser vi ces to gain access t o gover nment applications if such access i s not required by t heir or gani zational responsi bilities or there i s an alternate means of access to the gover nment application.

c. **Minimalism** – Identity Provider must transmit onl y t hose attribut es t hat are explicitly requested by t he Federal RP application or required by t he Federal identity asserti on profil e.

d. **Unique Identity --** Federal applications that do not require per sonall y identifiable identity i nfor mation (PII) must be gi ven a per si stent abstract identifier unique to the indi vidual Identity Subject. When allowed by t he technology, t he CSP mu st create a unique identifier for t he Identity Subject t hat i s al so unique to each Federal

appli cati on.

e. **No Activity Tracking** – CSPs must not di sclose infor mation regarding Identity

Subject activities with any Federal application to any ot her part y or use t he

infor mation for any purpose ot her t han problem resolution to support proper operation of the identity ser vice, or as r equired by law.

f. **Adequate Notice** – At t he ti me an Identit y Subject i nitiates access to a Fed eral gover nment application, that application may provi de text to be di splayed to the Subject before any PII is provided to the application by t he CSP. That text may include

• a general description of t he authentication event,

• any transaction( s) with the Federal applicati on,

• the pur pose of t he transaction( s),

• and a description of any di sclosure or transmi ssion of PII that will be r equested by t he Federal application.

The Subject should be allowed to cancel t he access transaction at thi s poi nt.

g. **Termination** – In the event an CSP ceases to provide t hi s ser vice, the Provi der shall conti nue to protect any sensiti ve data i ncludi ng PII and destroy it as soon as its preser vation i s no longer required by law or regulati on.

h. **Changes in the Service** – Should t he CSP alter the ter ms of use of t he servi ce, prompt noti ce mu st be provided to Identity Subject s. Such notice mu st i nclude a clear

deli neation of what ha s changed and the purpose of such cha nges.

i. **Dispute Resolution** – CSP’s mu st have a di spute resolution process for addressi ng any di sput e resulti ng from a co mplai nt filed by an Identity Subject utilizing its

ser vice who noti fi es t he CSP regardi ng a failure to comply wit h any ter ms in t he

CSP Service Definition required by t he SAC, and/or any additional criteria defined in t hi s Profile. The CSP must provi de evi dence to their Kant ara Initiati ve

132

133

134

135

136

137

138

Accredit ed Assessor both of t he exi stence of t hi s process and it s compliance t her eto.

j. **Technology Requirements –** CSP’s must be co mpliant with one or more of the ICAM-approved Aut hentication Schemes when engaged in any identity transaction wit h gover nment applications. (See [http://www.idmanagement.gov](http://www.idmanagement.gov/) for t he current li st of technology protocol s from whi ch to choo se.)