INCOMMON FEDERATION: PARTICIPANT OPERATIONAL PRACTICES

3DUWLFLSDWLRQ LQ WKH ,Q&RPPRQ)HGHUDWLRQ ´)HG participating organization ("Participant") to use Shibboleth identity attribute sharing technologies to manage access to online resources that can be made available to the InCommon community. One goal of the Federation is to develop, over time, community standards for such cooperating organizations to ensure that shared attribute assertions are sufficiently robust and trustworthy to manage access to important protected resources. As the community of trust evolves, the Federation expects that participants eventually should be able to trust each other's identity management systems and resource access management systems as they trust their own.

A fundamental expectation of Participants is that they provide authoritative and accurate attribute assertions to other Participants, and that Participants receiving an attribute assertion protect it and respect privacy constraints placed on it by the Federation or the source of that information. In furtherance of this goal, InCommon requires that each Participant make available to other Participants certain basic information about any identity management system, including the identity attributes that are supported, or resource access management system registered for use within the Federation.

Two criteria for trustworthy attribute assertions by Identity Providers are: (1) that the identity management system fall under the purview of t K H R U J D Q L] D W L R Q · V H [H

2.2 ´0HPEHU RI &RPPXQLW\µ Assertion: What subset of persons registered in your identity management system would you LGHQWLI\ DV D ´0HPEHU RI &RPPXQLW\µ LQ 6KLEEROHWK InCommon Participants?

Faculty, staff and active students

Electronic Identity Credentials

2.3 Please describe in general terms the administrative process used to establish an electronic identity that results in a record for that person being created in your electronic identity database. Please identify the office(s) of record for this purpose.)RU H[DPSOH ´5HJLVWUDU·V 2IILFH IRU VWXGHQWV +5 I

The Office for Student Assistance is responsible for collecting and managing student information. Faculty and staff information is managed by Human Resources. Student, faculty, and staff records are maintained in our University ERP database and electronic credentials (userids) are generated via an automated process based on the information contained in these records. This automated process is managed by Information Technology Services.

2.4 What technologies are used for your electronic identity credentials (e.g., Kerberos, userID/password, PKI, ...) that are relevant to Federation activities? If more than one type of electronic credential is issued, how is it determined who receives which type? If multiple credentials are linked, how is this managed (e.g., anyone with a Kerberos credential also can acquire a PKI credential) and recorded?

Kerberos, Active Directory

2.5 If your electronic identity credentials require the use of a secret password or PIN, and there are circumstances in which that secret would be transmitted across D QHWZRUN ZLWKRXW EHLQJ SURWHFWHG E\ HQFU\SWLRQ (e.g., used when accessing campus services), please identify who in your organization can discuss with any other Participant concerns that this might raise for them:

Our policy is to encrypt sensitive information such as authentication credentials.

2.6 ,I \RX VXSSRUW D ´6LQJOH 6LJQ2Q 6\VWHPµ across campus services (i.e., a single user authentication action to serve multiple applications, and you will make use of this to authenticate people for InCommon Service Providers, please describe the key security aspects of your SSO system including whether session

[4] "Member" is one possible value for eduPersonAffiliation as defined in the eduPerson schema. It is intended to include faculty, staff, student, and other persons with a basic set of privileges that go with PHPEHUVKLS LQ WKH XQLYHUVLW\ FRPPXQLW\ H J OLEUDU\ SULYLOHJ GHULYHG IURP RWKHU YDOXHV LQ HGX3HUVRQ$IILOLDWLRQ RU DVVLJQH identity database. See http://www.educause.edu/eduperson/

2.11 Would you consider your attribute assertions to be reliable enough to:

[X] control access to on-line information databases licensed to your organization?

[X] be used to purchase goods or services for your organization?

[X] enable access to personal information such as student loan status?

Privacy Policy

n (t)-3(i6e)h6 Teateour attr(-)34(lin)4 (e inf)5 (o)-ed (m)3 (ath-)-3 (e)t for c e15 (S)-52.ET667 ( )]TJ

2.11

Additional Notes and Details on the Operational Practices Questions

As a community of organizations willing to manage access to on-line resources cooperatively, and often without formal contracts in the case of non-commercial resources, it is essential that each Participant have a good understanding of the identity and resource management practices implemented by other Participants. The purpose of

Service Provider may be more willing to accept your assertions to the extent that this

applications for some period of time. This avoids people having to remember

[3.2] As a Service Provider, please declare what use(s) you would make of attribute information you receive.

[3.3] Personally identifying information can be a wide variety of things, not merely a name or credit card number. All information other than large group identity, e.g., ´PHPEHU RI FRPPXQLW\ µ VKRXOG EH SURWHFWHG ZKLOH

[3.4] Certain functional positions can have extraordinary privileges with respect to information on your systems. What oversight means are in place to ensure incumbents do not misuse such privileges?

[3.5] Occasionally protections break down and information is compromised. Some states have laws requiring notification of affected individuals. What legal and/or institutional policies govern notification of individuals if information you hold is compromised?

[4.1] Most InCommon Participants will use Internet2 Shibboleth technology, but this is not required. It may be important for other participants to understand whether you are using other implementations of the technology standards.

[4.2] As an Identity Provider, you may wish to place constraints on the kinds of applications that may make use of your assertions. As a Service Provider, you may wish to make a statement about how User credentials must be managed. This question is completely open ended and for your use.