eduPersonAnalyticsID

(defined in eduPerson-TBD); OID: 1.3.6.1.4.1.5923.1.1.1.17

RFC4512 definition

( 1.3.6.1.4.1.5923.1.1.1.17
NAME 'eduPersonAnalyticsID'
DESC 'Arbitrary reporting value associated with a subject or transaction'
EQUALITY caseIgnoreMatch
SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )

Application utility class: extended; # of values: multi

Definition

An opaque string that represents the use of a service by a subject for the purpose of
reporting or analytics by the originating organization.

When service access is anonymous or pseudonymous, a subject's home organization may
need the ability to summarize and analyze the use of a service without explicitly recording
that information at the point of access. This attribute allows for data to be provided to a
service at the point of access so that it can be compiled for reporting or other purposes by
the service.


A value consists of 1 to 127 ASCII characters, each of which is either an alphanumeric ASCII
character, the @ symbol (ASCII 64), an equals sign (ASCII 61), a hyphen (ASCII 45), an
underscore (ASCII 95), or a period (ASCII 46). The first character MUST be alphanumeric.

The ABNF [RFC2234] grammar is therefore:

<value> = (ALPHA / DIGIT) 0*126(ALPHA / DIGIT / "@" / "=" / "-" / "_" / ".")

Value comparison MAY be performed case-insensitively (that is, values that differ only by
case may be aggregated when reporting).

Notes

40     Granularity of the values SHOULD be coarse enough to prevent unintentional identification
41     of subjects or correlation of access to multiple services, but is not otherwise constrained
42     except by syntax.
43
44     The values SHOULD NOT be interpreted by a consuming service other than as opaque values
45     to be matched for the intended reporting function.
46
47     This attribute MUST NOT be used to make authorization decisions.
48
49     The mechanism by which the usage reports are provided to an organization is outside the
50     scope of this specification.
51
52     This attribute may or may not be stored in a typical Directory Service because of its potential
53     variance by service, but it is defined here for use in other contexts such as Security Assertion
54     Markup Language (SAML) assertions or OpenID Connect tokens. It is typically used in
55     federated scenarios in which anonymous or pseudonymous access is more frequent.
56
57     It is RECOMMENDED, if stored in an LDAP or X.500 directory, that the value be encoded
58     together with the identifier for a service (or set of services), in the form <value>|<service>
59     (separated by a pipe (ASCII 124). This facilitates ease of lookup of the values for a particular
60     service and encourages interoperability in software that needs to consume such data.
61
62     Examples
63
64     SAML:
65
66     <saml:Attribute Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.17"
67     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
68     FriendlyName="eduPersonAnalyticsID">
69     <saml:AttributeValue>FOOBAR_ZORKMID</saml:AttributeValue>
70     </saml:Attribute>
71
72     LDAP:
73     eduPersonAnalyticsID:FOOBAR_ZORKMID|https://sp.example.org/sp