Australian Government
Digital Transformation Agency

Attribute Profile

Trusted Digital Identity Framework
March 2018, version 0.6

CONSULTATION DRAFT

dta

Digital Transformation Agency

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968* and the rights explicitly granted below, all rights are reserved.

Licence

With the exception of the Commonwealth Coat of Arms and where otherwise noted, this product is provided under a Creative Commons Attribution 4.0 International Licence. (http://creativecommons.org/licenses/by/4.0/legalcode)

This licence lets you distribute, remix, tweak and build upon this work, even commercially, as long as they credit the DTA for the original creation. Except where otherwise noted, any reference to, reuse or distribution of part or all of this work must include the following attribution:

Trusted Digital Identity Framework: Attribute Profile © Commonwealth of Australia (Digital Transformation Agency) 2018

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the It's an Honour website (http://www.itsanhonour.gov.au)

Contact us

Digital Transformation Agency is committed to providing web accessible content wherever possible. If you are having difficulties with accessing this document, or have questions or comments regarding this document please email the Director, Trusted Digital Identity Framework at identity@dta.gov.au.

Document Management

This document has been reviewed and endorsed by the following groups.

Endorsement

Group	Endorsement date
Director, Trusted Digital Identity Framework	Mar 2018
Commonwealth GovPass Design Authority	

Change log

Version	Date	Author	Description of the changes
0.1	Jan 18	TM	Initial version
0.2	Jan 18	TM	Revision prior to release for comment.
0.3	Feb 18	TM	Revision to align with Trust Framework release 2.
0.3	Feb 18	TM	Revision from internal review.
0.5	Mar 18	TM	Added auth_time, tdif_audit_id attributes. Revised examples.
0.6	Mar 18	TM	Moved to updated TDIF template.

Conventions

The following conventions[1] are used in this document.

- **MUST** – means an absolute requirement of this document.
- **MAY** – means truly optional.

[1] These conventions are taken from Request for Comments 2119 (RFC2119) – Keywords for use in RFCs to indicate requirements levels

Contents

1 Introduction 1

2 Logical Attribute Profile 3

2.1 Overview 3

2.2 Identity Attributes 3

2.2.1 Attribute Data Representation 4

2.2.2 Attribute Sets 5

2.2.3 Attribute Sharing Policies 5

2.2.4 Levels of Assurance 6

3 Technical Attribute Profiles 8

3.1 OpenID Connect 1.0 Attribute Profile 8

3.1.1 Mapping attributes to OIDC 8

3.1.2 Design Goals 8

3.1.3 OIDC Attribute Mapping 9

3.2 SAML 2.0 Attribute Profile 11

3.2.1 Mapping attributes to SAML 2.0 11

3.2.2 Design Goals 11

3.2.3 SAML 2.0 Attribute Mapping 11

3.3 SAML 2.0 and OpenID Connect 1.0 Attribute Equivalents 12

References 14

Annex A - attribute examples 15

1 Introduction

The Digital Transformation Agency (DTA), in collaboration with other government agencies and key private sector bodies, is leading the development of a national federated identity 'eco-system' (the 'identity federation'). Implementation and operation of the identity federation is underpinned by the Trusted Digital Identity Framework (TDIF). This document should be read in conjunction with the *Trust Framework: Overview and Glossary*, which provides a high-level overview of the TDIF including its scope and objectives, the relationship between its various documents and the definition of key terms.

This document forms part of the technical integration standards that support the TDIF. It specifies the following:

- The logical attributes that are shared between Relying Parties and Identity Service Providers (IdP) via an Identity Exchange.
- Any policies that govern the sharing of these attributes, such requirements for user consent.
- The technical specifications for these logical attributes.
- The mapping of these attributes to the federation standards that used to share these attributes.

This document will be updated in future versions of the Trusted Digital Identity Framework as additional attributes are identified.

The document provides attribute mappings for the following federation standards:

- Open ID Connect 1.0.
- SAML 2.0.

This document should be the read in conjunction with the following technical integrations standards:

- *Trust Framework: OpenID Connect 1.0 Profile*
- *Trust Framework: SAML 2.0 Profile*

The intended audience for this document includes:

- Accredited Providers.
- Applicants.

- Authorised Assessors.
- Relying Parties.
- Trust Framework Accreditation Authority.

2 Logical Attribute Profile

2.1 Overview

The core identity attributes of a person's identity are their full name and date of birth. An IdP may be integrated with a Credential Service Provider (CSP) that will generally also use a verified email address and/or mobile phone number to manage a user's credentials, and these may also be shared with Relying Parties (RP). The verified indicators are used for conformance with the OpenID Connect 1.0 standard, these attributes should not be made available from an IdP unless they are verified.

Core identity attributes are populated from the identity documents that used by an IdPs to verify the identity attributes.

Additional attributes will be added in the future to support the need of RPs. Some attributes are mandatory and must be provided by an IdP, some attributes are optional.

2.2 Identity Attributes

Table 1 lists the identity attributes that defined by the TDIF. These attributes are sourced from an IdP.

An IdP:

- **MUST** provide a mandatory attribute.
- **MAY** provide an optional attribute.

An Identity Exchange **MUST** support the sharing of all attributes.

Table 1: Trust Framework identity attributes

Attribute	Description	Mandatory/ Optional
Family Name	Person's family name.	Mandatory
Given Names	Person's given names. There may be zero or more names separated by a space.	Mandatory
Date of Birth	Person's date of birth.	Mandatory
Email	Verified Email address	Optional

Attribute	Description	Mandatory/ Optional
Email Verified Indicator	Indicator whether the email address has been verified as being valid and belongs to the user. Always true.	Optional
Mobile Phone Number	Verified Mobile Phone Number.	Optional
Mobile Phone Number Verified	Indicator whether the mobile phone number has been verified as being valid and belongs to the user. Always true.	Optional
Authentication Time	Timestamp of when the person was authenticated at the Identity Provider.	Mandatory

Additional attributes may be supplied by an Identity Exchange to support the operation of the digital identity ecosystem.

Table 2 lists the additional attributes that an Identity Exchange may provide to a RP in response to a request.

An Identity Exchange:

- **MUST** provide a mandatory attribute.
- **MAY** provide an optional attribute.

Table 2: additional Relying Party attributes

Attribute	Description	Mandatory/ Optional
RP Audit Id	A unique identifier for every logical interaction between a Relying Party and an Identity Exchange to enable an audit trail. This attribute is generated by an Identity Exchange, made available to a Relying Party. It is never shared with an Identity Provider.	Mandatory

2.2.1 Attribute Data Representation

The data representation of TDIF attributes is detailed in Table 3.

Table 3: Trust Framework attribute data representation

Attribute	Type	Format	Maximum Length
Family Name	String	1 or more characters	100
Given Names	String	0 or more characters	100
Date of Birth	String	ISO 8601:2004 [ISO 8601:2004] format: YYYY-MM-DD. Note partial dates are also valid, i.e. YYYY, YYYY-MM	10
Email	String	Email address conforming to RFC 5322 [RFC 5322] address syntax	255

Attribute	Type	Format	Maximum Length
Email Verified Indicator	String	Boolean value of true/false	
Mobile Phone Number	String	Mobile phone number in E.164 [E.164] format.	15
Mobile Phone Number Verified	String	Boolean value of true/false	
Authentication Time	Datetime	Timestamp is protocol specific	
RP Audit Id	String	Universally Unique Identifier (UUID) conforming to RFC 4122 [RFC 4122].	36

2.2.2 Attribute Sets

Not all attributes are requested individually by a RP. Attribute sets correspond to the sets of attributes that a relying party will typically ask for as a collection, and that a user will provide consent for as a collection. Some attribute sets will contain a single attribute and some will contain a number of attributes.

Table 4: Trust Framework attribute sets

Attribute Set	Attributes	Description
Core	Family Name Given Name Date of Birth	The core identity data - name and date of birth. This attribute set only includes the current verified name. It includes the following attributes:
Email	Email Email Verified Indicator	Email address and an indicator as to whether it has been verified or not. It includes the following attributes
Phone	Mobile Phone Number Mobile Phone Number Verified	Mobile phone number and an indicator as to whether it has been verified or not
Common	RP Audit Id Authentication Time	Common attributes that are not specific to an Attribute Set.

2.2.3 Attribute Sharing Policies

Attribute Sharing Policies are applied to Attribute Sets and enforced by an Identity Exchange. These policies describe the rules that must be applied when sharing these attributes with RP. The key element of these policies relate to the operation of user consent. The different types of consent are detailed in Table 5. The TDIF may require additional policy requirements that must be enforced by an Identity Exchange. An example is attributes that are only available to specific RPs.

136 **Table 5:** Consent Types

Consent Type	Description
None	User consent not required for the attribute set.
Every Login	User consent is required for the attribute set every time a user authenticates
Every Change	User consent is required for the attribute set every time an attributes has changed. To meet this requirement the attribute set must contain a timestamp attribute.
Once	User consent for the attribute is required at least the first time it is shared. The user then has the option for this consent to be remembered.

137 An Identity Exchange **MUST** implement the attribute sharing policies that are detailed
138 in Table 6.

139 **Table 6:** attribute sharing policies

Attribute Set	Consent Requirement	Additional Policy Requirements
Core	Once	None
Email	Once	None
Mobile Phone Number	Once	None
Common	None	None
Levels Of Assurance	None	None

140 2.2.4 Levels of Assurance

141 Levels of Assurance (LoA) are special attributes used to describe the level of
142 assurance described in the TDIF.

143 **Table 7:** Trust Framework Levels of Assurance

LofA	Description
Identity Proofing Level of Assurance (IP)	Level of identity assurance associated with the core identity attributes. There are four levels of identity proofing assurance defined in the Trust Framework.
Credential Level of Assurance (CL)	Levels indicate the strength of the credential used to authenticate. There are three levels of credential assurance defined in the Trust Framework.

144 The LoAs are represented using values of an Authentication Context Class
145 Reference, commonly referred to as an acr. The concept of Authentication Context
146 Class is defined in both the SAML 2.0 and OpenID Connect 1.0 standards. In the
147 TDIF technical integration standards URNs are used to define each of the assurance
148 levels. The URNs are the valid combinations of the Identity Proofing LoA and

Credential Level LoA defined by the TDIF. A request for a valid combination in the table below is also satisfied by any combination that is ranked higher than it.

Table 8: Level of Assurance Combinations

Identity Proofing LoA	Credential Level LoA	URN	Ranking
IP1	CL1	`urn:id.gov.au:tdif:acr:ip1:cl1`	1
	CL2	`urn:id.gov.au:tdif:acr:ip1:cl2`	2
	CL3	`urn:id.gov.au:tdif:acr:ip1:cl3`	3
IP2	CL2	`urn:id.gov.au:tdif:acr:ip2:cl2`	4
	CL3	`urn:id.gov.au:tdif:acr:ip2:cl3`	5
IP3	CL2	`urn:id.gov.au:tdif:acr:ip3:cl2`	6
	CL3	`urn:id.gov.au:tdif:acr:ip3:cl3`	7
IP4	CL3	`urn:id.gov.au:tdif:acr:ip4:cl3`	8

3 Technical Attribute Profiles

The technical attribute profiles provide the mapping of the logical attributes to the federation protocols used by the TDIF technical integration standards. Attribute profiles are provided for the following standards:

- OpenID Connect 1.0 (OIDC)
- SAML 2.0

3.1 OpenID Connect 1.0 Attribute Profile

3.1.1 Mapping attributes to OIDC

Broadly speaking:

- Attributes corresponds to claims in OIDC
- Attribute Sets correspond to scopes in OIDC

3.1.2 Design Goals

The design goals for mapping the Attribute Profile to the OIDC specification are summarised for IdPs and RPs below:

3.1.2.1 Design goals for IDPs

The key design goals for the OIDC attribute mapping for IdPs are:

- Conform to standards.
- Use custom claims and scopes for TDIF-specific attributes to avoid conflicts with any other uses of the attributes, and the limit the data being returned from an IdP.
- Support extensibility by allowing additional claims and scopes can be easily added as the attributes handled by an Identity Exchange is expanded.

3.1.2.2 Design goals for RPs

The key design goals for the OIDC attribute mapping for RPs are:

- Maximise interoperability to simplify onboarding of RPs.

- Use commonly implemented features of the standards.
- Minimise the use of extensions to the standards.

3.1.3 OIDC Attribute Mapping

Table 9 describes the mapping of the TDIF attributes to OIDC claims. All claims are standard OIDC claims with the exception of `tdif_audit_id`. For standard claims a reference to the applicable section of the OpenID Connect 1.0 Core standard [OpenID.Core] is provided.

Table 9: OIDC Attribute Mapping

Attribute	OIDC Claim	JSON Type	OIDC Standard Reference
Family Name	`family_name`	`string`	Section 5.1
Given Names	`given_name`	`string`	Section 5.1
Date of Birth	`birthdate`	`string`	Section 5.1
Email	`email`	`string`	Section 5.1
Email Verified Indicator	`email_verified`	`boolean`	Section 5.1
Mobile Phone Number	`phone_number`	`string`	Section 5.1
Mobile Phone Number Verified	`phone_number_verified`	`boolean`	Section 5.1
Authentication Time	`auth_time`	`number`	Section 2
RP Audit Id	`tdif_audit_id`	`string`	

3.1.3.1 OIDC Attribute Profile for RPs

3.1.3.1.1 OIDC Scopes

Maps the TDIF attribute sets to the scopes that a RP may use to request identity attributes from an Identity Exchange. Claims are made available as follows:

- Via an ID Token from the Token Endpoint.
- Via the UserInfo Endpoint.

Claims will generally be available via both endpoints, future iterations of this attribute profile may restrict the availability of these claims if required.

An Identity Exchange **MUST** support all these scopes.

193 **Table 10:** OIDC Attribute Profile for RPs

Attribute Set	OIDC Scope	OIDC Claims	OIDC Claims Support	Comments

Core	`profile`	`family_name`
		`given_names`
		`birthdate`
			ID Token
			UserInfo
				Standard scope. Only the claims noted are returned.

Email	`email`	`email` `email_verified`	ID Token UserInfo	
Phone	`phone`	`phone_number` `phone_number_verified`	ID Token UserInfo	
Common	`*`	`tdif_audit_id`	ID Token	These attributes are returned for any scope requested

194 ### *3.1.3.2 OIDC Attribute Profile for IdPs*

195 #### *3.1.3.2.1 OIDC Scopes*

196 Table 11 maps the TDIF attribute sets to the scopes that an Identity Exchange may
197 use to request identity attributes from an IdP. Claims are made available as follows:

198 - Via an ID token from the Token Endpoint.
199 - Via the UserInfo Endpoint.

200 Claims will generally be available via both endpoints, future iterations of this attribute
201 profile may restrict the availability of these claims if required.

202 An Identity Provider **MUST** support all these scopes.

203 **Table 11:** OIDC Profile for IdPs

Attribute Set	OIDC Scope	OIDC Claims	OIDC Claims Support	Comments

Core	`tdif_core`	`family_name`
		`given_names`
		`birthdate`
			ID Token
			UserInfo
				Custom scope.

Email	`email`	`email` `email_verified`	ID Token UserInfo	Custom scope
Phone	`phone`	`phone_number` `phone_number_verified`	ID Token UserInfo	Custom scope

3.2 SAML 2.0 Attribute Profile

3.2.1 Mapping attributes to SAML 2.0

The SAML 2.0 Attribute Profile defines the expression of TDIF attributes as SAML attribute names and values.

3.2.2 Design Goals

The design goals for the SAML 2.0 attribute mapping are summarised below:

- Simplify protocol translation between OIDC and SAML by an Identity Exchange. Provide straightforward correspondence between the OIDC and SAML profile.
- Simplify interoperability. Avoid the use of custom SAML extensions, use standard built-in XML schema types, and where possible use the XML string data type.
- Provide the same functionality for Relying Parties regardless of the protocol being used.

3.2.3 SAML 2.0 Attribute Mapping

This profile defines the mapping of the Trust Framework attributes into specific attribute names. There is no concept of a scope in SAML 2.0.

In general, attributes are included in SAML 2.0 assertion about a subject in an `<AttributeStatement>` that contains an `<Attribute>` element for each attribute. See Section 2.7.3.1 of the SAML core specification [SAMLCore] . The following rules applies for the attributes returned as `<Attribute>` elements:

- The NameFormat XML attribute in `<Attribute>` elements MUST have the value `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`.
- A value of the XML attribute FriendlyName is provided for each of the SAML 2.0 attributes in this profile. This only defined for the purposes of readability, it is optional, and it plays no role in processing.
- The XML schema type of the contents of the `<AttributeValue>` must be drawn from one of the types defined Section 3 of [Schema2]. The xsi:type must be present and given the appropriate value.

The Authentication Time attributes uses the standard SAML `AuthnInstant` attribute in authentication responses. The time value is encoded in UTC. See Section 2.7.2 of the SAML core specification [SAMLCore] .

An Identity Exchange **MUST** support all attributes, with the exception of the RP Audit Id attributes.

An IdP **MUST** support all attributes.

Table 12: SAML 2.0 Attribute Mapping

Attribute	SAML Attribute Name	FriendlyName	XML Type
Family Name	urn:id.gov.au:tdif:family_name	family_name	string
Given Names	urn:id.gov.au:tdif:given_names	given_names	string
Date of Birth	urn:id.gov.au:tdif:birthdate	birthdate	string
Email	urn:id.gov.au:tdif:email	email	string
Email Verified Indicator	urn:id.gov.au:tdif:email_verified	email_verified	boolean
Mobile Phone Number	urn:id.gov.au:tdif:phone_number	phone_number	string
Mobile Phone Number Verified	urn:id.gov.au:tdif:phone_number_verified	phone_number_verified	boolean
RP Audit Id	urn:id.gov.au:tdif:tdif_audit_id	audit_id	string
Authentication Time	AuthnInstant		datetime

3.3 SAML 2.0 and OpenID Connect 1.0 Attribute Equivalents

Table 13 details the equivalent attributes in SAML 2.0 and OpenID 1.0 Connect for the Trust Framework attributes.

Table 13: SAML 2.0 and OIDC Attribute Equivalents

Attribute	OIDC Claim Name	SAML Attribute Name
Family Name	family_name	urn:id.gov.au:tdif:family_name
Given Names	given_name	urn:id.gov.au:tdif:given_names
Date of Birth	birthdate	urn:id.gov.au:tdif:birthdate
Email	email	urn:id.gov.au:tdif:email
Email Verified Indicator	email_verified	urn:id.gov.au:tdif:email_verified

Attribute	OIDC Claim Name	SAML Attribute Name
Mobile Phone Number	`phone_number`	`urn:id.gov.au:tdif:phone_number`
Mobile Phone Number Verified	`phone_number_verified`	`urn:id.gov.au:tdif:phone_number_verified`
Authentication Time	`auth_time`	`AuthInstant` attribute in the `<AuthnStatement>` element
RP Audit Id	`tdif_audit_id`	`urn:id.gov.au:tdif:tdif_audit_id`

243

References

The following information sources have been used in developing this document.

Table 14: References

Reference	
[E.164]	International Telecommunication Union, 2010, *E.164: The international public telecommunication numbering plan*, https://www.itu.int/rec/T-REC-E.164-201011-I/en
[ISO8601-2004]	International Organization for Standardization, 2004*, ISO 8601:2004. Data elements and interchange formats - Information interchange - Representation of dates and times*,
[RFC2119]	Bradner, S., *Key words for use in RFCs to Indicate Requirements Level*, RFC 2119, Internet Engineering Task Force, March 1997, https://tools.ietf.org/html/rfc2119
[RFC4122]	Leach, P., Mealling, M., Salz, R., *A Universally Unique IDentifier (UUID) URN Namespace*, RFC 4122, Internet Engineering Task Force, July 2005, https://tools.ietf.org/html/rfc4122
[RFC5322]	Resnick, P., Ed., Internet Message Format, RFC 5322, October 2008
[OpenID.Core]	Sakimura, N., Bradley, J., Jones, M., de Medeiros, B. and C. Mortimore*, OpenID Connect Core 1.0*, August 2015, http://openid.net/specs/openid-connect-core-1_0.html
[SAMLCore]	S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID samlcore-2.0-os. http://www.oasis-open.org/committees/security/
[Schema1]	H. S. Thompson et al. *XML Schema Part 1: Structures. World Wide Web Consortium Recommendation*, May 2001. See http://www.w3.org/TR/xmlschema-1/. Note that this specification normatively references [Schema2], listed below
[Schema2]	Paul V. Biron, Ashok Malhotra. *XML Schema Part 2: Datatypes. World Wide Web Consortium Recommendation*, May 2001. See http://www.w3.org/TR/xmlschema-2/.

Annex A - attribute examples

Table 15 below provides an example of each TDIF attribute in SAML 2.0 and OIDC.

Table 15: SAML and OIDC attribute examples

Attribute	Examples

Family Name	Example SAML Value:
	`<saml:Attribute`
	`NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" Name="urn.id.gov.au:tdif:family_name" FriendlyName="family_name"> <saml:AttributeValue xsi:type="xs:string">Moore</saml:AttributeValue>`
	`</saml:Attribute>`
	
	Example OIDC Value:
	`"family_name": "Moore"`

Given Names	Example SAML Value:
	`<saml:Attribute`
	`NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" Name="urn.id.gov.au:tdif:given_names" FriendlyName="given_names"> <saml:AttributeValue xsi:type="xs:string">Trentino</saml:AttributeValue>`
	`</saml:Attribute>`
	
	Example JWT Value:
	`"given_name": "Trentino"`

Date of Birth	Example OIDC Value:
	`<saml:Attribute`
	`NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" Name="urn.id.gov.au:tdif:birthdate" FriendlyName="birthdate">`
	`<saml:AttributeValue xsi:type="xs:string">1972-05-06</saml:AttributeValue>`
	`</saml:Attribute>`
	
	Example OIDC Value:
	`"birthdate": "1972-05-06"`

Email	Example SAML Value:
	`<saml:Attribute`
	`NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" Name="urn.id.gov.au:tdif:email" FriendlyName="email">`
	`<saml:AttributeValue xsi:type="xs:string">tmoore@foobar.com.au</saml:AttributeValue>`
	`</saml:Attribute>`
	
	Example OIDC Value:
	`"email": "tmoore@foobar.com.au"`

Email Verified Indicator	Example SAML Value: `<saml:Attribute`

Attribute	Examples
	NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri” Name=”urn.id.gov.au:tdif:email_verified” FriendlyName=”email_verified”> <saml:AttributeValue xsi:type="xs:boolean">true</saml:AttributeValue> </saml:Attribute> Example OIDC Value: "email_verified": true
Mobile Phone Number	Example SAML Value: <saml:Attribute NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri” Name=”urn.id.gov.au:tdif:phone_number_verified” FriendlyName=”phone_number”> <saml:AttributeValue xsi:type="xs:string">+61444888222</saml:AttributeValue> </saml:Attribute> Example OIDC Value: "phone_number": “+61444888222”
Mobile Phone Number Verified	Example SAML Value: <saml:Attribute NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri” Name=”urn.id.gov.au:tdif:phone_number_verified” FriendlyName=”phone_number_verified”> <saml:AttributeValue xsi:type="xs:boolean">true</saml:AttributeValue> </saml:Attribute> Example OIDC Value: "phone_number_verified": true
RP Audit Id	Example SAML Value: <saml:Attribute NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri” Name=”urn.id.gov.au:tdif:tdif_audit_id” FriendlyName=”audit_id”> <saml:AttributeValue xsi:type="xs:string">AA97B177-9383-4934-8543-0F91A7A02836</saml:AttributeValue> </saml:Attribute> Example OIDC Value: "tdif_audit_id": “AA97B177-9383-4934-8543-0F91A7A02836”
Authentication Time	Example SAML Value: <saml:AuthnStatement AuthnInstant="2018-03-05T03:20:48Z">> <saml:AuthnContext> <saml:AuthnContextClassRef>urn:id.gov.au:tdif:acr:ip3:cl2</saml:AuthnContextClassRef> </saml:AuthnContext> </saml:AuthnStatement>

Attribute	Examples
	Example OIDC Value: `"auth_time": 1520220048`

251