Sistema di autenticazione federata del cittadino (AdC)

Linee guida di integrazione delle applicazioni

Sommario

Attributi di integrazione per l'autenticazione federata 2
Applicazioni SAML2 compliant: link utili per l'integrazione 2
Applicazioni non SAML2 compliant 3
Informazioni comuni a tutte le applicazioni 4

Attributi di integrazione per l'autenticazione federata

Gli attributi del token SAML2 scambiato con l'applicazione, sono gli attributi che l'applicazione avrà a disposizione nell'header HTML.

IMPORTANTE:
1. nell'header non sarà disponibile nessun altro parametro;
2. l'unico attributo sempre presente è il CodiceFiscale; la presenza degli altri attributi non è certa e dipendente dalle informazioni presenti in LDAP.

Significato	**Attributo SAML**	**Obbligatorietà**
Nome	nome	
Cognome	cognome	
Titolo di studio	titolo	
Codice Fiscale	CodiceFiscale	X
Sesso ("M" o "F")	sesso	
Data di nascita (formato dd/MM/yyyy)	dataNascita	
Luogo di nascita	luogoNascita	
Provincia di nascita (valorizzato con il codice della provincia)	provinciaNascita	
Stato di nascita	statoNascita	
Indirizzo e-mail utilizzato dall'infrastruttura per le comunicazioni ufficiali al cittadino. Dovrebbe corrispondere ad una casella di tipo PEC	emailAddress	
Viene posto uguale a emailAddress	emailAddressPersonale	
Numero di cellulare	cellulare	
Numero di telefono	telefono	
Indirizzo domicilio	capDomicilio	
	cittaDomicilio	
	indirizzoDomicilio	
	provinciaDomicilio	
	statoDomicilio	
Indirizzo residenza	capResidenza	
	cittaResidenza	
	indirizzoResidenza	
	provinciaResidenza	
	statoResidenza	
Certificato X509 (valorizzato solo per autenticazioni con smart-card)	x509certificate_subjectdn	
	x509certificate_issuerdn	
	x509certificate_base64	

Applicazioni SAML2 compliant: link utili per l'integrazione

URL dei metadati forniti dalla federazione:
https://idp-test.infotn.it/icar-lp/metadata
https://adc.provincia.tn.it/icar-lp/metadata

URL per il login:
https://adc.provincia.tn.it/idp/Authn/UnifiedLogin

L'applicazione dovrà fornire un URL per lo scarico dei metadati utili per l'integrazione nella federazione.

Applicazioni non SAML2 compliant

Alle applicazioni che non sono in grado di integrarsi direttamente al sistema di autenticazione federata, ma che sono proxabili attraverso i proxy di Informatica Trentina, Informatica Trentina mette a disposizione direttamente sui proxy le funzionalità di comunicazione SAML2.
All'applicazione verranno inviati gli attributi del token SAML2 attraverso attributi dell'header http secondo la mappatura seguente:

Attributo SAML	**Nome nell'header http**
nome	givenname
cognome	surname
titolo	titolo
CodiceFiscale	codicefiscale
sesso	sesso
dataNascita	nascitadata
luogoNascita	nascitaluogo
provinciaNascita	nascitaprovincia
statoNascita	nascitastato
emailAddress	email
emailAddressPersonale	emailpersonale
cellulare	cellulare
telefono	telefono
capDomicilio	domiciliocap
cittaDomicilio	domiciliocitta
indirizzoDomicilio	domicilioindirizzo
provinciaDomicilio	domicilioprovincia
statoDomicilio	domiciliostato
capResidenza	residenzacap
cittaResidenza	residenzacitta
indirizzoResidenza	residenzaindirizzo
provinciaResidenza	residenzaprovincia
statoResidenza	residenzastato
x509certificate_subjectdn	x509subjectdn
x509certificate_issuerdn	x509issuerdn
x509certificate_base64	x509base64

Oltre agli attributi del token SAML2, nell'header http verranno opzionalmente popolati i seguenti attributi:

Attributo nell'header HTTP	**Significato**	**Esempio**
Shib-Cookie-Name		
Shib-Session-ID		

Shib-Session-Index		
Shib-Identity-Provider	Nome dell'identity provider	https://adc.provincia.tn.it/idp/shibboleth
Shib-Authentication-Method	Metodo di autenticazione usato	
Shib-Authentication-Instant	Giorno e ora di autenticazione	2015-05-21T07:03:35.601Z
Shib-AuthnContext-Class	Classe utilizzata per l'autenticazione	urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard
Shib-AuthnContext-Decl		
Shib-Assertion-Count		
Shib-Application-ID	Identificativo dell'applicazione	

Informazioni comuni a tutte le applicazioni

Url per il logout da integrare nell'applicazione:
https://idp-test.infotn.it/icar-lp/Logout
https://adc.provincia.tn.it/icar-lp/Logout
Poiché il sistema di autenticazione federata del cittadino fornisce nativamente la funzionalità di single sign-on web la chiamata alla logout si tradurrà per l'utente nel logout da tutte le applicazioni presenti nella medesima sessione del browser.

Applicazioni di prova disponibili:
https://idp-test.infotn.it/jee-sp-test/