SPID Quality Assessment Document

Checklist per la verifica dell'implementazione SPID dei Service Provider

DATA: 11/03/2019 VERSIONE 1.0

Version History

VERSIONE	AUTORE	STATO	MODIFICHE
1.0	AGID	PUBBLICATO	

SPID Quality Assessment Document

Checklist per la verifica dell'implementazione SPID dei Service Provider

Il presente documento contiene l'elenco dei test che permettono di valutare il livello di conformità dell'implementazione di un Service Provider alle regole tecniche SPID. I test di seguito indicati sono gli stessi eseguiti da AgID, tramite il tool SPID SAML Check, per la verifica tecnica dell'implementazione, come descritto nella procedura tecnica sul sito spid.gov.it.
Il documento vuole essere uno strumento utile ai Service Provider per effettuare i necessari test di conformità prima di richiedere la verifica tecnica ad AgID.

Test sulla correttezza del Metadata

strict : Test the compliance of AssertionConsumerService element(s)

Num	Descrizione	Esito
1.1.0	At least one AssertionConsumerService must be present	
1.1.1	The index attribute must be present	
1.1.2	The index attribute must be >= 0	
1.1.3	The Binding attribute must be present	
1.1.4	The Binding attribute must be one of [urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST, urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect	
1.1.5	The Location attribute must be present	
1.1.6	The Location attribute must be a valid HTTPS url	
1.1.7	Only one default AssertionConsumerService must be present	
1.1.8	Must be present the default AssertionConsumerService with index = 0	

strict : Test the compliance of AttributeConsumingService element(s)

Num	Descrizione	Esito
1.2.0	One or more AttributeConsumingService elements must be present	
1.2.1	The index attribute in AttributeConsumigService element must be present	
1.2.2	The index attribute in AttributeConsumigService element must be >= 0	
1.2.3	The ServiceName element must be present	
1.2.4	The ServiceName element must have a value	
1.2.5	One or more RequestedAttribute elements must be present	
1.2.6	The Name attribute in RequestedAttribute element must be present	
1.2.7	The Name attribute in RequestedAttribute element must be one of [address, companyName, countyOfBirth, dateOfBirth, digitalAddress, email,	

	expirationDate, familyName, fiscalNumber, gender, idCard, ivaCode, mobilePhone, name, placeOfBirth, registeredOffice, spidCode]	
1.2.8	The Name attribute in RequestedAttribute element must be present	
1.2.9	The Name attribute in RequestedAttribute element must be one of [address, companyName, countyOfBirth, dateOfBirth, digitalAddress, email, expirationDate, familyName, fiscalNumber, gender, idCard, ivaCode, mobilePhone, name, placeOfBirth, registeredOffice, spidCode]	
1.2.10	The Name attribute in RequestedAttribute element must be present	
1.2.11	The Name attribute in RequestedAttribute element must be one of [address, companyName, countyOfBirth, dateOfBirth, digitalAddress, email, expirationDate, familyName, fiscalNumber, gender, idCard, ivaCode, mobilePhone, name, placeOfBirth, registeredOffice, spidCode]	
1.2.12	The Name attribute in RequestedAttribute element must be present	
1.2.13	The Name attribute in RequestedAttribute element must be one of [address, companyName, countyOfBirth, dateOfBirth, digitalAddress, email, expirationDate, familyName, fiscalNumber, gender, idCard, ivaCode, mobilePhone, name, placeOfBirth, registeredOffice, spidCode]	
1.2.14	The Name attribute in RequestedAttribute element must be present	
1.2.15	The Name attribute in RequestedAttribute element must be one of [address, companyName, countyOfBirth, dateOfBirth, digitalAddress, email, expirationDate, familyName, fiscalNumber, gender, idCard, ivaCode, mobilePhone, name, placeOfBirth, registeredOffice, spidCode]	
1.2.16	The Name attribute in RequestedAttribute element must be present	
1.2.17	The Name attribute in RequestedAttribute element must be one of [address, companyName, countyOfBirth, dateOfBirth, digitalAddress, email, expirationDate, familyName, fiscalNumber, gender, idCard, ivaCode, mobilePhone, name, placeOfBirth, registeredOffice, spidCode]	
1.2.18	The Name attribute in RequestedAttribute element must be present	
1.2.19	The Name attribute in RequestedAttribute element must be one of [address, companyName, countyOfBirth, dateOfBirth, digitalAddress, email, expirationDate, familyName, fiscalNumber, gender, idCard, ivaCode, mobilePhone, name, placeOfBirth, registeredOffice, spidCode]	
1.2.20	The Name attribute in RequestedAttribute element must be present	
1.2.21	The Name attribute in RequestedAttribute element must be one of [address, companyName, countyOfBirth, dateOfBirth, digitalAddress, email, expirationDate, familyName, fiscalNumber, gender, idCard, ivaCode, mobilePhone, name, placeOfBirth, registeredOffice, spidCode]	
1.2.22	The Name attribute in RequestedAttribute element must be present	
1.2.23	The Name attribute in RequestedAttribute element must be one of [address, companyName, countyOfBirth, dateOfBirth, digitalAddress, email, expirationDate, familyName, fiscalNumber, gender, idCard, ivaCode, mobilePhone, name, placeOfBirth, registeredOffice, spidCode]	
1.2.24	The Name attribute in RequestedAttribute element must be present	
1.2.25	The Name attribute in RequestedAttribute element must be one of [address, companyName, countyOfBirth, dateOfBirth, digitalAddress, email, expirationDate, familyName, fiscalNumber, gender, idCard, ivaCode, mobilePhone, name, placeOfBirth, registeredOffice, spidCode]	

1.2.26	The Name attribute in RequestedAttribute element must be present	
1.2.27	The Name attribute in RequestedAttribute element must be one of [address, companyName, countyOfBirth, dateOfBirth, digitalAddress, email, expirationDate, familyName, fiscalNumber, gender, idCard, ivaCode, mobilePhone, name, placeOfBirth, registeredOffice, spidCode]	

strict : Test the compliance of EntityDescriptor element

Num	Descrizione	Esito
1.3.0	Only one EntityDescriptor element must be present	
1.3.1	The entityID attribute must be present	
1.3.2	The entityID attribute must have a value	

strict : Test the compliance of KeyDescriptor element(s)

Num	Descrizione	Esito
1.4.0	At least one signing KeyDescriptor must be present	
1.4.1	At least one signing x509 must be present	
1.4.2	At least one encryption x509 must be present	

strict : Test the compliance of Organization element

Num	Descrizione	Esito
1.5.0	Only one Organization element can be present	
1.5.1	One or more OrganizationName elements must be present	
1.5.2	The lang attribute in OrganizationName element must be present	
1.5.3	The OrganizationName element must have a value	
1.5.4	One or more OrganizationDisplayName elements must be present	
1.5.5	The lang attribute in OrganizationDisplayName element must be present	
1.5.6	The OrganizationDisplayName element must have a value	
1.5.7	One or more OrganizationURL elements must be present	
1.5.8	The lang attribute in OrganizationURL element must be present	
1.5.9	The OrganizationURL element must have a value	
1.5.10	The OrganizationURL element must be a valid URL	

strict : Test the compliance of SPSSODescriptor element

Num	Descrizione	Esito
1.6.0	Only one SPSSODescriptor element must be present	
1.6.1	The protocolSupportEnumeration attribute must be present	
1.6.2	The protocolSupportEnumeration attribute must have a value	
1.6.3	The AuthnRequestsSigned attribute must be present	
1.6.4	The AuthnRequestsSigned attribute must have a value	
1.6.5	The AuthnRequestsSigned attribute must be true	

strict : Test the compliance of Signature element

Num	Descrizione	Esito
1.7.0	The Signature element must be present	
1.7.1	The SignatureMethod element must be present	
1.7.2	The Algorithm attribute must be present in SignatureMethod element	
1.7.3	The signature algorithm must be one of [http://www.w3.org/2001/04/xmldsig-more#ecdsasha256, http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha384, http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512, http://www.w3.org/2001/04/xmldsig-more#hmac-sha256, http://www.w3.org/2001/04/xmldsig-more#hmac-sha384, http://www.w3.org/2001/04/xmldsig-more#hmac-sha512, http://www.w3.org/2001/04/xmldsig-more#rsa-sha256, http://www.w3.org/2001/04/xmldsigmore#rsa-sha384, http://www.w3.org/2001/04/xmldsig-more#rsa-sha512]	
1.7.4	The DigestMethod element must be present	
1.7.5	The Algorithm attribute must be present in DigestMethod element	
1.7.6	The digest algorithm must be one of [http://www.w3.org/2001/04/xmlenc#sha256, http://www.w3.org/2001/04/xmlenc#sha384, http://www.w3.org/2001/04/xmlenc#sha512]	

strict : Test the compliance of SingleLogoutService element(s)

Num	Descrizione	Esito
1.8.0	One or more SingleLogoutService elements must be present	
1.8.1	The Binding attribute in SingleLogoutService element must be present	
1.8.2	The Binding attribute in SingleLogoutService element must have a value	
1.8.3	The Binding attribute in SingleLogoutService element must be one of [urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST, urn:oasis:names:tc:SAML:2.0:bindings:HTTPRedirect	
1.8.4	The Location attribute in SingleLogoutService element must be present	
1.8.5	The Location attribute in SingleLogoutService element must have a value	
1.8.6	The Location attribute in SingleLogoutService element must be a valid URL	

strict : Verify the SP metadata signature

Num	Descrizione	Esito
1.9.0	the metadata signature must be valid	

strict : Validate the SP metadata against the SAML 2.0 Medadata XSD

Num	Descrizione	Esito
1.10.0	the metadata must validate against the XSD	

Test sulla correttezza della AuthnRequest

strict : Test the compliance of AuthnRequest element

Num	Descrizione	Esito
2.1.0	One AuthnRequest element must be present	
2.1.1	The ID attribute must be present	
2.1.2	The ID attribute must have a value	
2.1.3	The Version attribute must be present	
2.1.4	The Version attribute must be 2.0	
2.1.5	The IssueInstant attribute must be present	
2.1.6	The IssueInstant attribute must have a value	
2.1.7	The IssueInstant attribute must be a valid UTC string	
2.1.8	The Destination attribute must be present	
2.1.9	The Destination attribute must have a value	
2.1.10	The Destination attribute must be a valid HTTPS url	
2.1.11	The IsPassive attribute must not be present	
2.1.12	The AssertionConsumerServiceURL attribute must be present	
2.1.13	The AssertionConsumerServiceURL attribute must have a value	
2.1.14	The AssertionConsumerServiceURL attribute must be a valid HTTPS url	
2.1.15	The ProtocolBinding attribute must be present	
2.1.16	The ProtocolBinding attribute must have a value	
2.1.17	The ProtocolBinding attribute must be urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST	
2.1.18	The AttributeConsumingServiceIndex attribute must have a value	
2.1.19	The AttributeConsumingServiceIndex attribute must be >= 0	

strict : Test the compliance of Issuer element

Num	Descrizione	Esito
2.2.0	One Issuer element must be present	
2.2.1	The Issuer element must have a value	
2.2.2	The Format attribute must be present	
2.2.3	The Format attribute must have a value	
2.2.4	The Format attribute must be urn:oasis:names:tc:SAML:2.0:nameid-format:entity	
2.2.5	The NameQualifier attribute must be present	
2.2.6	The NameQualifier attribute must have a value	

strict : Test the compliance of NameIDPolicy element

Num	Descrizione	Esito
2.3.0	One Issuer element must be present	

2.3.1	The AllowCreate attribute must not be present	
2.3.2	The Format attribute must be present	
2.3.3	The Format attribute must have a value	
2.3.4	The Format attribute must be urn:oasis:names:tc:SAML:2.0:nameid-format:transient	

strict : Test the compliance of RequestedAuthnContext element

Num	Descrizione	Esito
2.4.0	Only one RequestedAuthnContex element must be present	
2.4.1	The Comparison attribute must be present	
2.4.2	The Comparison attribute must have a value	
2.4.3	The Comparison attribute must be one of [exact, minimum, better, maximum]	
2.4.4	Only one AuthnContexClassRef element must be present	
2.4.5	The AuthnContexClassRef element must have a value	
2.4.6	The AuthnContextClassRef element must have a valid SPID level	

strict : Test the compliance of RequesterID element

Num	Descrizione	Esito
2.5.0	The RequesterID element must not be present	

strict : Test the compliance of Scoping element

Num	Descrizione	Esito
2.6.0	The Scoping element must not be present	

strict : Test the compliance of Signature element

Num	Descrizione	Esito
2.7.0	The Signature element must be present	
2.7.1	The SignatureMethod element must be present	
2.7.2	The Algorithm attribute must be present in SignatureMethod element	
2.7.3	The signature algorithm must be one of ['http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256', 'http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha384', 'http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512', 'http://www.w3.org/2001/04/xmldsig-more#hmac-sha256', 'http://www.w3.org/2001/04/xmldsig-more#hmac-sha384', 'http://www.w3.org/2001/04/xmldsig-more#hmac-sha512', 'http://www.w3.org/2001/04/xmldsig-more#rsa-sha256', 'http://www.w3.org/2001/04/xmldsig-more#rsa-sha384', 'http://www.w3.org/2001/04/xmldsig-more#rsa-sha512']	
2.7.4	The DigestMethod element must be present	

2.7.5	The Algorithm attribute must be present in DigestMethod element	
2.7.6	The digest algorithm must be one of ['http://www.w3.org/2001/04/xmlenc#sha256', 'http://www.w3.org/2001/04/xmlenc#sha384', 'http://www.w3.org/2001/04/xmlenc#sha512']	

strict : Test if the XSD validates and if the signature is valid

Num	Descrizione	Esito
2.8.0	The AuthnRequest must validate against XSD and must have a valid signature	

Test sulla correttezza del SP alla ricezione della Response

I seguenti casi di test servono a valutare il comportamento del Service Provider in relazione alla possibile Response ricevuta dall'IdP. Il risultato atteso è indicato nella rispettiva colonna.

Num	Descrizione	Risultato atteso	Esito
3.1	Response corretta	OK	
3.2	Response non firmata	Errore	
3.3	Response - Assertion non firmata	Errore	
3.4	Response - Firma non valida	Errore	
3.8	Response - ID non specificato	Errore	
3.9	Response - ID mancante	Errore	
3.10	Response - Version diverso da 2.0	Errore	
3.11	Response - IssueInstant non specificato	Errore	
3.12	Response - IssueInstant mancante	Errore	
3.13	Response - Formato IssueInstant non corretto	Errore	
3.14	Response - IssueInstant precedente Request	Errore	
3.15	Response - IssueInstant successivo Request	Errore	
3.16	Response - InResponseTo non specificato	Errore	
3.17	Response - InResponseTo mancante	Errore	
3.18	Response - InResponseTo diverso da Request	Errore	
3.19	Response - Destination non specificato	Errore	
3.20	Response - Destination mancante	Errore	
3.21	Response - Destination diverso da AssertionConsumerServiceURL	Errore	
3.22	Response - Elemento Status non specificato	Errore	
3.23	Response - Elemento Status mancante	Errore	
3.24	Response - Elemento StatusCode non specificato	Errore	
3.25	Response - Elemento StatusCode mancante	Errore	
3.26	Response - Elemento StatusCode diverso da success (non valido)	Errore	
3.27	Response - Elemento Issuer non specificato	Errore	
3.28	Response - Elemento Issuer mancante	Errore	
3.29	Response - Elemento Issuer diverso da EntityID IdP	Errore	
3.30	Response - Attributo Format di Issuer diverso	Errore	
3.31	Response - Autenticazione annullata da IdP	Errore	
3.32	Response - Elemento Assertion mancante	Errore	
3.33	Assertion - Attributo ID non specificato	Errore	
3.34	Assertion - Attributo ID mancante	Errore	
3.35	Assertion - Attributo Version diverso da 2.0	Errore	
3.36	Assertion - Attributo IssueInstant non specificato	Errore	
3.37	Assertion - Attributo IssueInstant mancante	Errore	
3.38	Assertion - Attributo IssueInstant avente formato non corretto	Errore	
3.39	Assertion - Attributo IssueInstant precedente a IssueInstant della Request	Errore	
3.40	Assertion - Attributo IssueInstant successivo a IssueInstant della Request	Errore	

3.41	Assertion - Elemento Subject non specificato	Errore	
3.42	Assertion - Elemento Subject mancante	Errore	
3.43	Assertion - Elemento NameID non specificato	Errore	
3.44	Assertion - Elemento NameID mancante	Errore	
3.45	Assertion - Attributo Format di NameID non specificato	Errore	
3.46	Assertion - Attributo Format di NameID mancante	Errore	
3.47	Assertion - Attributo Format di NameID diverso	Errore	
3.48	Assertion - Attributo NameQualifier di NameID non specificato	Errore	
3.49	Assertion - Attributo NameQualifier di NameID mancante	Errore	
3.51	Assertion - Elemento SubjectConfirmation non specificato	Errore	
3.52	Assertion - Elemento SubjectConfirmation mancante	Errore	
3.53	Assertion - Attributo Method di SubjectConfirmation non specificato	Errore	
3.54	Assertion - Attributo Method di SubjectConfirmation mancante	Errore	
3.55	Assertion - Attributo Method di SubjectConfirmation diverso	Errore	
3.56	Assertion - Elemento SubjectConfirmationData mancante	Errore	
3.57	Assertion - Attributo Recipient di SubjectConfirmationData non specificato	Errore	
3.58	Assertion - Attributo Recipient di SubjectConfirmationData mancante	Errore	
3.59	Assertion - Attributo Recipient di SubjectConfirmationData diverso	Errore	
3.60	Assertion - Attributo InResponseTo di SubjectConfirmationData non specificato	Errore	
3.61	Assertion - Attributo InResponseTo di SubjectConfirmationData mancante	Errore	
3.62	Assertion - Attributo InResponseTo di SubjectConfirmationData diverso da ID request	Errore	
3.63	Assertion - Attributo NotOnOrAfter di SubjectConfirmationData non specificato	Errore	
3.64	Assertion - Attributo NotOnOrAfter di SubjectConfirmationData mancante	Errore	
3.65	Assertion - Attributo NotOnOrAfter di SubjectConfirmationData avente formato non corretto	Errore	
3.66	Assertion - Attributo NotOnOrAfter di SubjectConfirmationData precedente all'istante di ricezione della response	Errore	
3.67	Assertion - Elemento Issuer non specificato	Errore	
3.68	Assertion - Elemento Issuer mancante	Errore	
3.69	Assertion - Elemento Issuer diverso da EntityID IdP	Errore	
3.70	Assertion - Attributo Format di Issuer non specificato	Errore	
3.71	Assertion - Attributo Format di Issuer mancante	Errore	
3.72	Assertion - Attributo Format di Issuer diverso	Errore	
3.73	Assertion - Elemento Conditions non specificato	Errore	
3.74	Assertion - Elemento Conditions mancante	Errore	
3.75	Assertion - Attributo NotBefore di Condition non specificato	Errore	
3.76	Assertion - Attributo NotBefore di Condition mancante	Errore	

3.77	Assertion - Attributo NotBefore di Condition avente formato non corretto	Errore	
3.78	Assertion - Attributo NotBefore di Condition successivo all'istante di ricezione della response	Errore	
3.79	Assertion - Attributo NotOnOrAfter di Condition non specificato	Errore	
3.80	Assertion - Attributo NotOnOrAfter di Condition mancante	Errore	
3.81	Assertion - Attributo NotOnOrAfter di Condition avente formato non corretto	Errore	
3.82	Assertion - Attributo NotOnOrAfter di Condition precedente all'istante di ricezione della response	Errore	
3.83	Assertion - Elemento AudienceRestriction di Condition non specificato	Errore	
3.84	Assertion - Elemento AudienceRestriction di Condition mancante	Errore	
3.85	Assertion - Elemento Audience di AudienceRestriction di Condition non specificato	Errore	
3.86	Assertion - Elemento Audience di AudienceRestriction di Condition mancante	Errore	
3.87	Assertion - Elemento Audience di AudienceRestriction di Condition diverso da Entity Id del Service Provider	Errore	
3.88	Assertion - Elemento AuthStatement non specificato	Errore	
3.89	Assertion - Elemento AuthStatement mancante	Errore	
3.90	Assertion - Elemento AuthnContext di AuthStatement non specificato	Errore	
3.91	Assertion - Elemento AuthnContext di AuthStatement mancante	Errore	
3.92	Assertion - Elemento AuthContextClassRef di AuthnContext di AuthStatement non specificato	Errore	
3.93	Assertion - Elemento AuthContextClassRef di AuthnContext di AuthStatement mancante	Errore	
3.94	Assertion - Elemento AuthContextClassRef impostato su https://www.spid.gov.it/SpidL1	In base alla Request	
3.95	Assertion - Elemento AuthContextClassRef impostato su https://www.spid.gov.it/SpidL2	In base alla Request	
3.96	Assertion - Elemento AuthContextClassRef impostato su https://www.spid.gov.it/SpidL3	In base alla Request	
3.97	Assertion - Elemento AuthContextClassRef impostato ad un valore non previsto	Errore	
3.98	Assertion - Elemento AttributeStatement presente, ma sottoelemento Attribute mancante	Errore	
3.99	Assertion - Elemento AttributeStatement presente, con sottoelemento Attribute non specificato	Errore	
3.100	Assertion - Firma diversa	Errore	
3.103	Assertion - Set di attributi inviato diverso da quello richiesto	Errore	
3.104	Anomalie utente - Ripetuta sottomissione di credenziali errate (Anomalia 19)	Errore. Viene segnalato l'errore come da tabelle anomalie SPID	

3.105	Anomalie utente - Utente privo di credenziali compatibili (Anomalia 20)	Errore. Viene segnalato l'errore come da tabelle anomalie SPID	
3.106	Anomalie utente - Timeout (Anomalia 21)	Errore. Viene segnalato l'errore come da tabelle anomalie SPID	
3.107	Anomalie utente - Consenso negato (Anomalia 22)	Errore. Viene segnalato l'errore come da tabelle anomalie SPID	
3.108	Anomalie utente - Credenziali bloccate (Anomalia 23)	Errore. Viene segnalato l'errore come da tabelle anomalie SPID	
3.109	Attributi senza NameFormat	Errore	