Regione Toscana

Settore Sanita’ digitale e innovazione

Cornice di sicurezza per i servizi REST sanità di RT

Specifiche tecniche ver. 1.4

Note versione

Numero	Data	Autore	Note
1.0	16.07.2024	G. Ugolini O. Lorenzini	• Prima emissione
1.1	19.09.2024	G. Ugolini O. Lorenzini	• Inserito elemento obbligatorio iat
1.2	30.09.2024	G. Ugolini O. Lorenzini	• Cambiato CN del certificato
1.3	01.10.2024	G. Ugolini O. Lorenzini	• Cambiato esempio header token jwt
1.4	10.10.2024	G. Ugolini O. Lorenzini	• Integrazione query • verifica integrità payload • adottato pattern di sicurezza INTEGRITY_REST_01 • adeguato esempio

Indice generale

1 Scopo del documento

Scopo di questo documento è la definizione di una cornice di sicurezza finalizzata alla interoperabilità del Sistema Informativo Sanitario e Sociosanitario (SIS) di Regione Toscana con i corrispondenti sistemi Territoriali .
Il documento fa riferimento agli standard MODI definiti da Agid [1].
La sicurezza è pertanto assicurata dalla crittografazione del canale di colloquio tra fruitore ed erogatore e dalla produzione di token jwt all'interno dell'header http . Di seguito il dettaglio della specifica che comunque riferisce per i dettagli agli standard MODI .

2 Sicurezza Canale

La sicurezza della trasmissione e identificazione del soggetto mittente è assicurata dalla adozione del profilo ID_AUTH_CHANNEL_02 . Ad ogni fruitore viene pertanto fornito una credenziale di autenticazione basata su certificati X.509 . Il certificato viene fornito da Regione Toscana a valle di una richiesta di adesione al servizio.
Il CN sarà generalmente così valorizzato :
A (AUTH)
N (progressivo) -
Codice Regione Codice Azienda
Dominio : come da indicazioni di compliance
NomeFornitore: Nome del fornitore
Identificativo della struttura utente : Codifica HSP.11 - HSP.11bis - STS.11 - RIA.11. \ Nel caso di ruolo APR assume il valore del codice ISTAT dell'Azienda (ASL) . Riferimento: urn:oasis:names:tc:xspa:1.0:environment:locality

Esempio:A1-090904SIADGPI9061401

3 Sicurezza Messaggio

Si richiede l'invio di un token JWS nell'header RTSAN-JWT-Signature che deve essere prodotto in conformità al pattern di sicurezza **INTEGRITY_REST_01 delle linee guida tecniche di interoperabilità** che estende [ID_AUTH_REST_02] Direct Trust con certificato X.509 su REST **.**

Si richiede inoltre che:

- il fruitore referenzi il certificato X.509 utilizzando il claim x5c (X.509 Certificate Chain).
- Si assume l'esistenza di un trust tra fruitore ed erogatore, che permette il riconoscimento da parte dell'erogatore del certificato X.509, o la CA emittente
- Il JSON del payload del token suddetto deve essere esteso con i claim obbligatori riportati nella tabella seguente.

ISSUER	Stringa che contiene il nome identificativo dell'entità che ha generato il token. Valorizzato con "auth:" seguito dal "Common Name del certificato di autenticazione "	auth:A1-090904SIADGPI9061401	Obbligatorio	iss
IAT	Numero intero (timestamp in secondi) che indica il momento in cui il token è stato generato, serve per conoscere l'età di un token	1540890704	Obbligatorio	iat
NBF	Numero intero (timestamp in secondi) per indicare l'istante di prima validità del token	1540890704	Non Obbligatorio	nbf
EXPIRATION	Numero intero (timestamp in secondi) che indica fino a quando il token sarà valido (5minuti)	1540918800	Obbligatorio	exp
ID_JWT	identificativo del JWT, per evitare replay attack	3190bfbc-858c-11ef-967b-005056865883	Obbligatorio	jti

AUDIENCE	Indica il destinatario per cui è stato creato il token, da valorizzare con la base URL del servizio, comprensivo della versione	https:// api.regione.toscana.it/sanita/ C01/SIAD/v1	Obbligatorio	aud
SERVICE_NAME	indica il nome del servizio applicativo interoperabile	SIAD	Obbligatorio	sn
SERVICE_VERSION	Indica la versione del servizio applicativo interoperabile	v1	Obbligatorio	sv
SUBJECT	Codice Fiscale dell'utente che fa richiesta del servizio di interoperabilità Formato codifica conforme alle specifiche IHE (ITI TF-3) **Vedi nota 1**	VRDMRC67T20I257E^^^&2.16.840.1.113883.2.9.4.3.2&ISO	Obbligatorio	sub
USER ID	un identificativo univoco dell'utente interno al dominio del fruitore che ha determinato l'esigenza della request di accesso all'e-service dell'erogatore ad esempio potrebbe essere il CF del medico o il nome del sw che fa la request verso l'erogatore	LRNMRO80A41C351J oppure nome dell'applicativo a valle del fruitore	Non Obbligatorio. Obbligatorio nel caso in cui l'erogatore richieda puntualmente chi ha fatto la request.	userID

USER LOCATION	un identificativo univoco della postazione interna al dominio del fruitore da cui è avviata l'esigenza della request di accesso all'e-service dell'erogatore	73.227.130.85 oppure nome_postazionelavoro CF del soggetto che opera	Non Obbligatorio. Obbligatorio nel caso in cui l'erogatore richieda puntualmente chi ha fatto la request	userLocation
IDENTIFICATIVO REGIONE	Identificativo regione mittente	090	Obbligatorio	subject_organization_id

STRUTTURA UTENTE	Identificativo della struttura utente. Codifica ISTAT della Azienda (ASL) concatenato alla codifica HSP.11 - HSP.11bis - STS.11 - RIA.11. \ Nel caso di ruolo APR assume il valore del codice ISTAT dell'Azienda (ASL) Le codifiche saranno ampliate per coprire tutte le casistiche mancanti. Riferimento: urn:oasis:names:tc:xspa:1.0:environment:locality	90400011A	Obbligatorio	locality
CONTESTO OPERATIVO RICHIESTA	Contesto operativo della richiesta	TREATMENT per l'invio UPDATE per la cancellazione e sostituzione QUERY per la richiesta di lettura	Obbligatorio	purpose_of_use

TIPO ATTIVITÀ	Descrive il tipo di attività	CREATE per invio DELETE per Eliminazione UPDATE per sostituzione GET per lettura	Obbligatorio	action_id
ID APPLICATIVO	ID applicativo dell'utente	Astercloud	Obbligatorio	subject_application_ id
VENDOR APPLICATIVO	Vendor applicativo dell'utente	GPI	Obbligatorio	subject_application_ vendor
VERSIONE APPLICATIVO	Versione applicativo dell'utente	v.1.2.3	Obbligatorio	subject_application_ version
SIGNED_HEADERS	Array contenente una lista di json objects per supportare la firma di più header ed eventualmente verificare il loro ordinamento	"signed_headers": [{ "digest": "SHA-256=AVRzYUoODDVP9tmC2JzDLW9inQBtalrJYvXJ/goxLts=" }, { "content-type": "application/json" }]	Obbligatorio nei casi in cui sia presente il payload	signed_headers
DIGEST	valore del Digest header dei representation data secondo le indicazioni in RFC 3230 questo serve per l'integrità della rappresentazione della risorsa	SHA256=AVRzYUoODDVP9tmC2JzDLW9inQBtalrJYvXJ/goxLts=	Obbligatorio nei casi in cui sia presente il payload	digest
CONTENT_TYPE	HTTP header Content-Type	application/json	Obbligatorio nei casi in cui sia presente il payload	content-type
CONTENT_ENCO	Indica la codifica	zip	Obbligatorio se è	content-encoding

DING	per payload		presente un payload che ha una codifica particolare	

Nota 1

IL SUBJECT rappresenta il CF

Codice Fiscale dell'utente che fa richiesta del servizio di interoperabilità

Formato codifica conforme alle specifiche IHE (ITI TF-3).

Ad Esempio inserire il CF del responsabile di struttura / dipartimento etc...

Nota 2

Rt fornisce un certificato da usare sia per la auth che per la sign.

4 Riferimenti

https://www.agid.gov.it/sites/default/files/repository_files/linee_guida_interoperabilit_tecnica_pa.pdf

NOTA: il documento PDF che descrive il pattern INTEGRITY_REST è incluso come allegato del pdf principale, come "Documento Operativo Pattern di Sicurezza". Nello specifico RT estende ID_AUTH_REST_02

5 Esempio

Quello che segue è un esempio di token che rispetta il formato descritto per la Cornice Sicurezza oggetto di specifica .


```
{
"alg": "RS256",
"typ": "JWT", "x5c": [
"**************************CERT*****************************"
]
}
{
  "iat": 1728402432,
  "nbf": 1728402432,
  "exp": 1728402732,
  "jti": "3190bfbc-858c-11ef-967b-005056865883",
  "aud": "https://apistage.regione.toscana.it/C06/rest/RegioneToscanaSanita/GrandiMacchinari/v1",
  "client_id": "GrandiMacchinari/v1",
  "iss": "auth:apigwstage.regione.toscana.it",
  "sub": "VRDMRC67T20I257E^^^&2.16.840.1.113883.2.9.4.3.2&ISO",
  "subject_organization_id": "090",
  "sv": "v1",
  "purpose_of_use": "treatment",
  "action_id": "create",
  "locality": "90400011A",
  "subject_application_id": "Astercloud",
  "sn": "CS_Test",
```

```
  "subject_application_version": "v.1.2.3",
  "subject_application_vendor": "GPI",
  "signed_headers": [
    {
      "digest": "SHA-256=AVRzYUoODDVP9tmC2JzDLW9inQBtalrJYvXJ/goxLts="
    },
    {
      "content-type": "application/json"
    }
  ]
}
```