ACCESSO SERVIZI MEDIR HTTPS

1 ABBREVIAZIONI E TERMINI

- CDA: Clinical Document Architecture
- HTTPS: HyperText Transfer Protocol over Secure Socket Layer
- MEDIR:Progetto Rete Dei Medici di Medicina Generale e Pediatri di Libera Scelta e Fascicolo Sanitario Elettronico (Medir)
- MMG: Medico di Medicina Generale: con questo termine si intendono i Medici di Assistenza Primaria, i Medici di Continuità Assistenziale, i Medici di Emergenza sanitaria territoriale, Medici della Dirigenza Medica Territoriale
- OID: Object IDentifier
- TSE: Tavolo di Sanità Elettronica
- RTI: Raggruppamento Temporaneo di Imprese
- SW: Software
- XML: Extensible Markup Language
- XSD: XML Schema Definition Language
- W3C: World Wide Web Consortium
- WSDL:Web Services Description Language

2 RIFERIMENTI

[1]. DocB-SpecificheIntegrazioneServiceGatewayWSDL

[2]. DocA-PianoIntegrazioneApplicativiCartellaClinica

[3]. DocC-Annex A-WDSL ServiziGatewayMedir

3 SCOPO DEL DOCUMENTO

Questo documento si basa specificamente sulla modalità di invocazione dei servizi Medir tramite protocollo di sicurezza HTTPS, andando così ad aggiungere uno strato di sicurezza nella comunicazione client server tramite la creazione di un canale criptato regolato da scambio certificati.

La modalità di accesso HTTPS lascia di fatto inalterati i servizi e le operazioni messi a disposizione dal sistema, ma anche la modalità di autenticazione WS_Trust che già in precedenza garantiva lo strato di sicurezza necessario tra comunicazioni Web Services.

Sia i Web Services che l'intero flusso di sicurezza WS-Trust sono descritti nel dettaglio nei documenti [1] e [2].

4 ADEGUAMENTO CONFIGURAZIONI CLIENT

L'applicazione del protocollo di crittografia è stato definito creando sul server che espone i punti di accesso ai servizi Medir, ovvero i servizi di Gateway, un certificato digitale con chiave pubblica e privata.

La chiave pubblica verrà fornita a tutte le società che si occupano di sviluppare i client di integrazione e di fatto costituisce il meccanismo di riconoscimento sul server per consentire lo scambio di messaggi ed il rilascio del token di autenticazione.

Lato client, di fatto, l'utilizzo della chiave pubblica in fase di presentazione ai servizi Medir, sostituisce i certificati server precedentemente forniti ed utilizzati prima per il rilascio token di sicurezza e successivamente per le comunicazioni server.

Per accedere ai servizi in modalità HTTPS è necessario configurare adeguatamente i binding del client con i puntamenti ai servizi HTTPS e specificando il certificato da utilizzare, tale configurazione può essere fatta manualmente, facendo riferimento ai WSDL estratti nel documento [3], o alternativamente andando a generare le service references dei servizi disponibili nei percorsi indicati.

- https://fse.sardegnasalute.it/GatewayWS/aslX/wsdl/DocumentRegistry/DocumentRegistryService.wsdl
- https://fse.sardegnasalute.it/GatewayWS/aslX/wsdl/DocumentRepository/DocumentRepositoryService.wsdl
- https://fse.sardegnasalute.it/GatewayWS/aslX/wsdl/PatientIdentity/PatientIdentity.wsdl
- https://fse.sardegnasalute.it/GatewayWS/aslX/wsdl/PersonnelManagement/PersonnelManagement.wsdl
- https://fse.sardegnasalute.it/GatewayWS/aslX/wsdl/NotificationBroker/NotificationBroker.wsdl
- https://fse.sardegnasalute.it/GatewayWS/aslX/wsdl/SubscriptionManager/SubscriptionManager.wsdl
- https://fse.sardegnasalute.it/GatewayWS/aslX/wsdl/SARBroker/SARBrokerINPS.wsdl

Per convenzione, nei percorsi indicati, "aslX" è un placeholder che in fase di configurazione deve essere sostituito con l'identificativo della ASL verso cui sta avvenendo il puntamento come da seguente esempio per la ASL1, si specifica inoltre che l'indirizzo indicato fa riferimento agli ambienti di integrazione e certificazione, ma nel caso di ambiente di produzione andrà modificato anche il nome host
https://fse.sardegnasalute.it/GatewayWS/asl1/wsdl/DocumentRegistry/DocumentRegistryService.wsdl

Gli indirizzi specificati sono relativi all'ambiente di test integrazioni e certificazione, i nomi dei servizi sono analoghi nell'ambiente di produzione gli unici accorgimenti da adottare in tale ambiente per raggiungere gli stessi servizi sono:

- utilizzare il corretto certificato server a livello di sistema operativo e bindings servizi
- utilizzare il nome host del certificato di produzione ovvero
  https://fse.sardegnasalute.it/GatewayWS/aslX/wsdl/DocumentRegistry/DocumentRegistryService.wsdl
- accertarsi che il path degli endpoint includa il corretto riferimento alla ASL utilizzata, esempio per ASL1
  https://fse.sardegnasalute.it/GatewayWS/asl1/wsdl/DocumentRegistry/DocumentRegistryService.wsdl

Di seguito un riepilogo dei servizi esposti dal Service Gateway di Medir e richiamabili da un client operatore sono quelli elencati nella seguente tabella:

Servizi esposti sul Gateway Medir	
Document Registry	«WSDLnamespace» DocumentRegistryService
Document Repository	«WSDLnamespace» DocumentRepositoryService
Anagrafe Asssistiti	«WSDLnamespace» PatientIdentity

Anagrafe Operatori	«WSDLnamespace» PersonnelManagement
Publish&Subscribe	«WSDLnamespace» NotificationBroker
Publish&Subscribe	«WSDLnamespace» SubscriptionManager
SARBroker	«WSDLnamespace» SARBrokerINPS

Per il dettaglio delle operazioni disponibili nei vari servizi si rimanda al documento [1] dove vengono riportate tutte le operation descritte nei vari servizi con i relativi diagrammi.

5 AMBIENTI E CERTIFICATI

Sono previsti gli ambienti di test certificazione e di produzione a cui è associato lo stesso certificato lato Server di cui viene distribuita la relativa chiave pubblica:

- "fse.sardegnasalute.it" è il certificato da utilizzare per l'accesso ai servizi, si tratta di un certificato rilasciato da una Certification Autorithy attendibile, pertanto in questo caso è necessario importare nel trust store del sistema operativo soltanto la chiave pubblica del certificato server

Si specifica che nel caso di accesso agli ambienti di test e certificazione sarà necessario configurare preventivamente la modalità di comunicazione tramite host mapping, questo perché il nome host non viene risolto pubblicamente, tali configurazioni saranno predisposte in fase di integrazione. Il fornitore dovrà indicare gli indirizzi IP da cui vorrà testare le funzionalità per poterlo abilitare all'accesso in questo ambiente.

Nell'ambiente di produzione, invece, essendo il nome host pubblicato su dns pubblico, l'indirizzo viene risolto senza alcuna ulteriore configurazione.