PKI Manager

IST.05.32 – Istruzione Operativa

Gestione certificati X509

LAZIOcrea S.p.A. – Società a Socio unico Regione Lazio – Cap. Soc. € 924.400,00
Sede legale e amministrativa: Via del Serafico, 107 00142 Roma - T +39 06 51563[illegible] F +39 06 51563611
C.F./P.IVA 13662331001 – R.E.A. RM-1464288
PEC Azienda: laziocrea@legalmail.it
www.laziocrea.it - www.regione.lazio.it

Status del Documento

Identificazione

Revisione	1.0		
Titolo	PKI Manager		
Tipo	Istruzione Operativa		
N. Pagine	15		
Classificazione LAZIOcrea	☐ Pubblico	☒ Interno	☐ Confidenziale
Status	☐ In lavorazione	☐ Bozza	☒ Pubblicato

INDICE

1. Introduzione 4
1.1 Scopo del documento 4
1.2 Siglario definizioni e riferimenti 4
1.3 Riferimenti 4
1.4 Termini chiave 5
2. Definizione del contesto 6
2.1 Certificati digitali e PKI 6
3. PKI Manager 8
Inserimento nuova richiesta 9
Elenco richieste 11
Revoca 13
Generazione file CSR 14
Esempio di generazione delle CSR mediante openssl 15

1. Introduzione

1.1 Scopo del documento

La presente istruzione operativa descrive le modalità di gestione del ciclo di vita di certificati X509.V3, emessi da una CA interna a beneficio delle esigenze progettuali del Fascicolo Sanitario Elettronico 2.0

Il documento espone i concetti di base della gestione di certificati digitali, aka PKI, la soluzione adottata nonché i casi d'uso di detta soluzione.

1.2 Siglario definizioni e riferimenti

Acronimo	Descrizione
AA	Attribute Authority
ABA	American Bar Association Digital Signature Guidelines
AIA	Authority Information Access
ASN.1	Abstract Syntax Notation One
CA	Certification Authority
CMC	Certificate Management Messages over CMS
CMS	Cryptographic Message Syntax
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
CSR	Certificate Signing Request
DER	Distinguished Encoding Rules
DSA	Digital Signature Algorithm
EDI	Electronic Data Interchange
LRA	Local Registration Authority
HSM	Hardware Security Module
IPRA	Internet Policy Registration Authority
ISP	Internet Service Provider
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PEM	Internet Privacy Enhanced Mail
PCA	Policy Certification Authorities
PKC	Public Key Certificate
PKI	Internet Public Key Infrastructure
RA	Registration Authority

1.3 Riferimenti

RFC5280	https://www.rfc-editor.org/rfc/rfc5280
ISO/IEC 9594-8:2020	https://www.iso.org/standard/80325.html
AGID-IntOpsSecure	https://www.agid.gov.it/sites/default/files/repository_files/linee_guida_tecnologie_e_standard_sicurezza_interoperabilit_api_sistemi_informatici.pdf

1.4 Termini chiave

Nel presente documento sono utilizzati i termini chiave “DEVE”, “NON DEVE”, “OBBLIGATORIO”, “VIETATO”, “DOVREBBE”, “CONSIGLIATO”, “NON DOVREBBE”, “SCONSIGLIATO”, “POTREBBE”, “OPZIONALE” in conformità a quanto specificato in RFC2119, e precisamente:

DEVE, OBBLIGATORIO	definiscono un requisito assoluto, la specifica deve essere implementata, la consegna è inderogabile
DOVREBBE, CONSIGLIATO	significano che in particolari circostanze possono esistere validi motivi per ignorare un requisito, non implementare una specifica, derogare alla consegna, ma che occorre esaminare e valutare con attenzione le implicazioni correlate alla scelta
PUÒ, OPZIONALE	definiscono che l’elemento della specifica è a implementazione facoltativa
NON DOVREBBE, SCONSIGLIATO	significano che in particolari circostanze possono esistere validi motivi per cui un elemento di specifica è accettabile o persino utile, ma, prima di implementarlo, le implicazioni correlate dovrebbero essere esaminate e valutate con attenzione
NON DEVE, VIETATO	significano che c’è proibizione assoluta di implementazione di un determinato elemento di specifica

2. Definizione del contesto

2.1 Certificati digitali e PKI

L'impiego di certificati digitali è una buona prassi per assicurare un adeguato livello di sicurezza nei diversi contesti informatizzati in rete.

Lo standard di riferimento per i certificati digitali è lo X.509, proposto dallo ITU-T (*International Telecommunication Union*) nel 1988, formalmente CCITT X.509, e ISO/IEC 9594-8, è uno standard consolidato nella sua versione 3 sin dal 1996.

Lo standard definisce il formato dei certificati a chiave pubblica (PKC) ed i ruoli delle Entità coinvolte nella gestione del ciclo di vita di un certificato.

Un certificato **X.509 v3** (RFC5280) è un formato standard per **certificati a chiave pubblica**, ovvero documenti digitali che associano in modo sicuro e fidato chiavi digitali a siti web, individui o organizzazioni. Il certificato a chiave pubblica rende possibile la crittografia asimmetrica basata sulla coppia di chiavi pubblica e privata.

I ruoli necessari a sostegno della gestione del ciclo di vita di un certificato sono altresì definiti dall standard e, complessivamente s'istanziano in una PKI (*public key infrastructure*) che attraverso processi e strumenti garantisce l'associazione dell'identità di un dato soggetto ad un certificato. I ruoli fondamentali di una PKI sono:

- ✓ la Certification Authority (CA) emette certificati, genera CRL, genera la coppia chiavi privata e pubblica, sulla base di una richiesta firmata (CSR aka PKCS#10) assicura l'unicità della chiave pubblica;
- ✓ la Root Authority è l'autorità radice di tutte le CA, certifica esclusivamente le altre CA;
- ✓ le Local Registration Authorities (LRA): alcune CA richiedono la presenza fisica dell'utente finale e quindi una LRA gioca il ruolo di intermediario, delegato al riconoscimento del soggetto.

Si riporta di seguito il diagramma, tratto dallo RFC5280, delle Entità di una PKI e le relative relazioni.

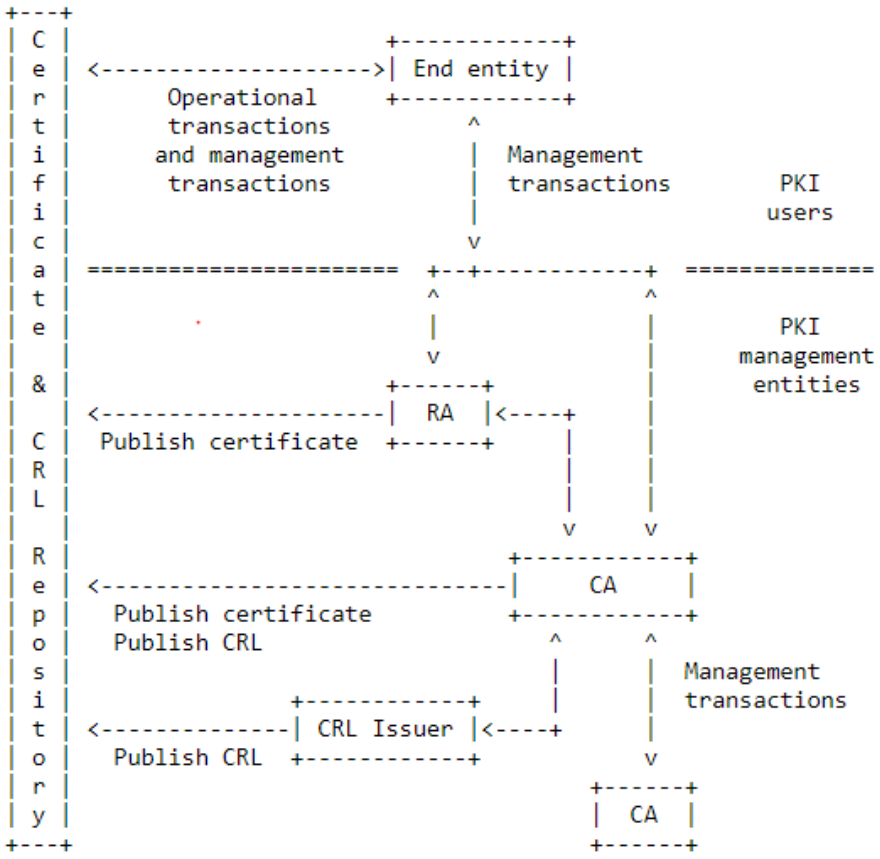


Figura 1: PKI Entity

Una PKI si fonda sul principo della fiducia attribuitagli dagli Utenti nell'assicurare in modo certo l'attribuzione di un generico soggetto ad una data chiave digitale; per tale scopo il processo di accreditamento dei prestatori di servizi fiduciari d'ambito pubblico è particolamente oneroso ed impegnativo.

Tuttavia, anche in considerazione di quanto specificato in [IntOpsSecure §6.2.2] fissando un dominio, ovvero perimetro d'interoperabilità ci si può avvalere di una PKI interna per l'emmissione, la distribuzione e la revoca di certificati X.509.

Si è pertanto realizzata una PKI interna avvalendosi della soluzione open source ejbca, per gestire in modo organico e governato l'emissione di certificati per uso interno, ovvero per un dato dominio d'interoperabilità, descritta nel seguito e con la specificazione delle operazioni supportate.

3. PKI Manager

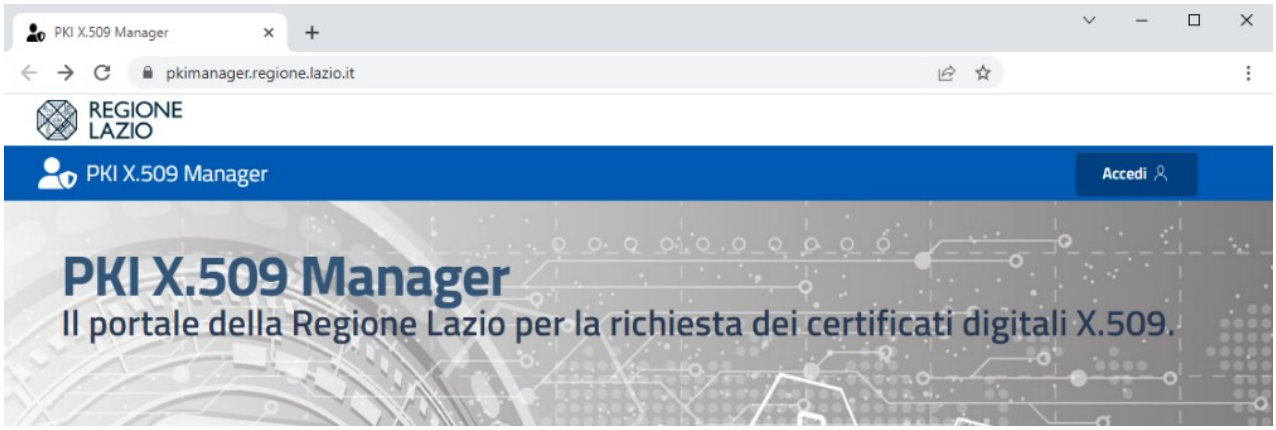
PKI Manger è la soluzione software realizzata da LazioCrea per l'amministrazione delle richieste di emissione/revoca/rinnovo dei certificati emessi dalla nostra PKI e utilizzati per scopi di

- Autenticazione/ Trasporto
- Firma

L'accesso al sistema è consentito solo tramite I&AM di Regione Lazio e nello specifico tramite SPID, CIE, TS-CNS, AzureAD (LDAP)

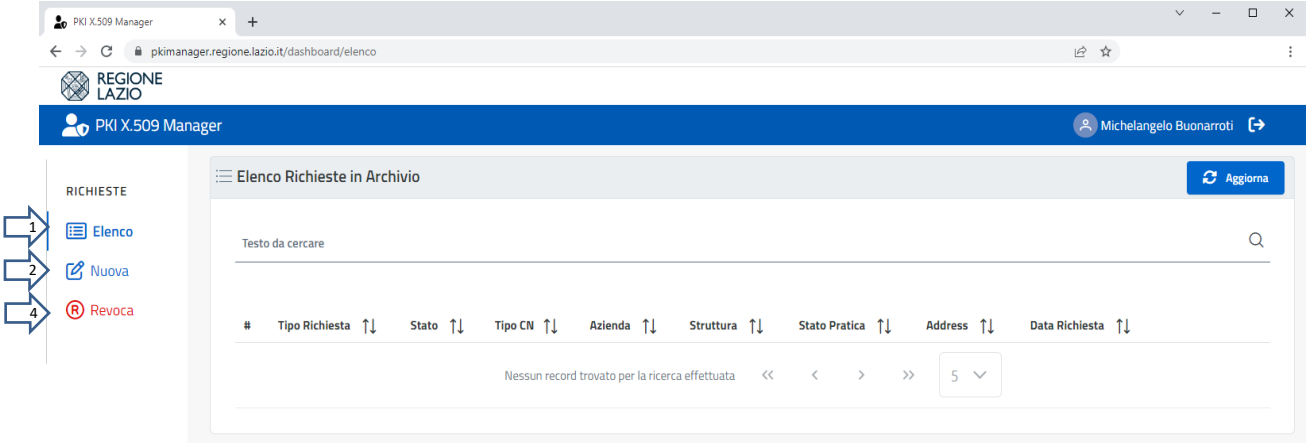
Il servizio è raggiungibile tramite la URL

https://pkimanager.regione.lazio.it/



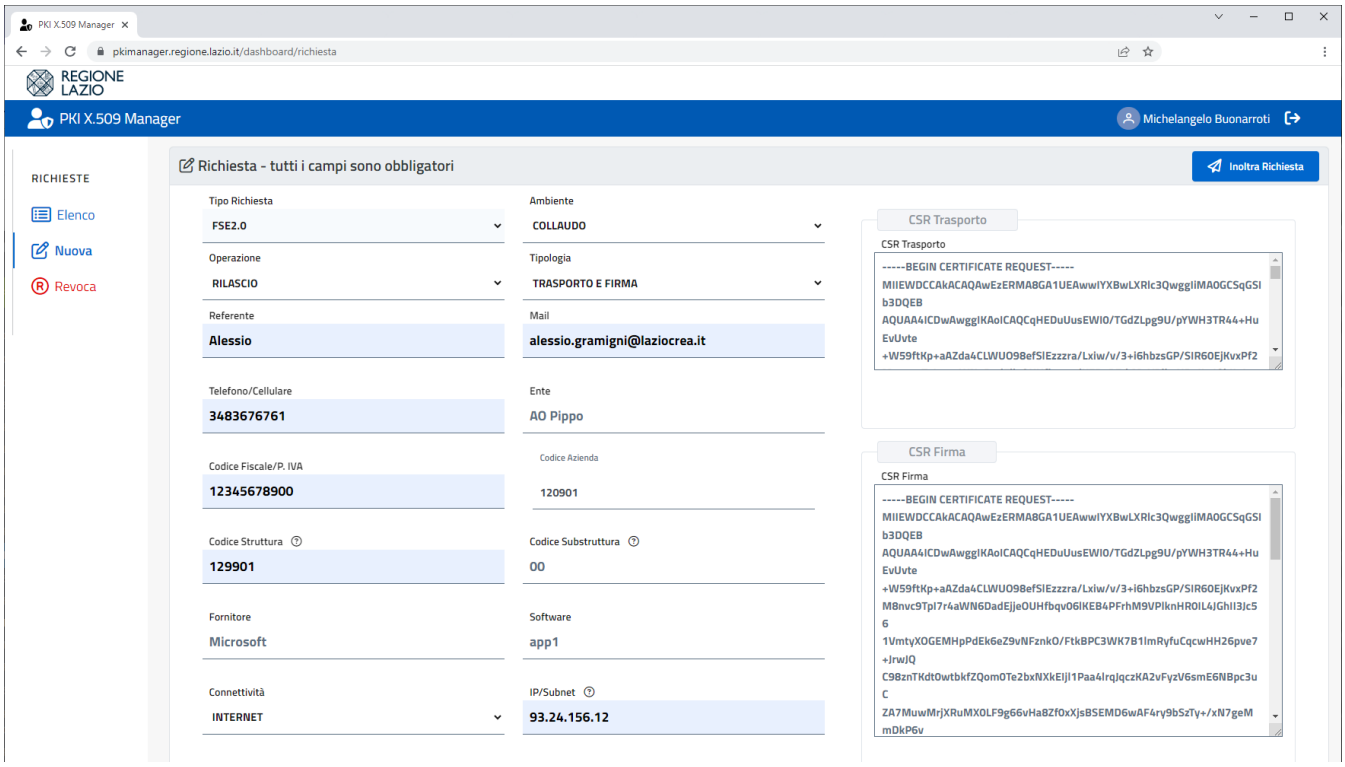
Una volta effettuato l'acceso sarà possibile

1. Controllare lo state delle richieste inserite vedendo nel dettaglio i dati inviati
2. Inserire una nuova richiesta di emissione
3. Richiedere la revoca di un certificato presente nella lista di quelli richiesti
4. Richiedere la revoca di un certificato emesso da terzi



Inserimento nuova richiesta

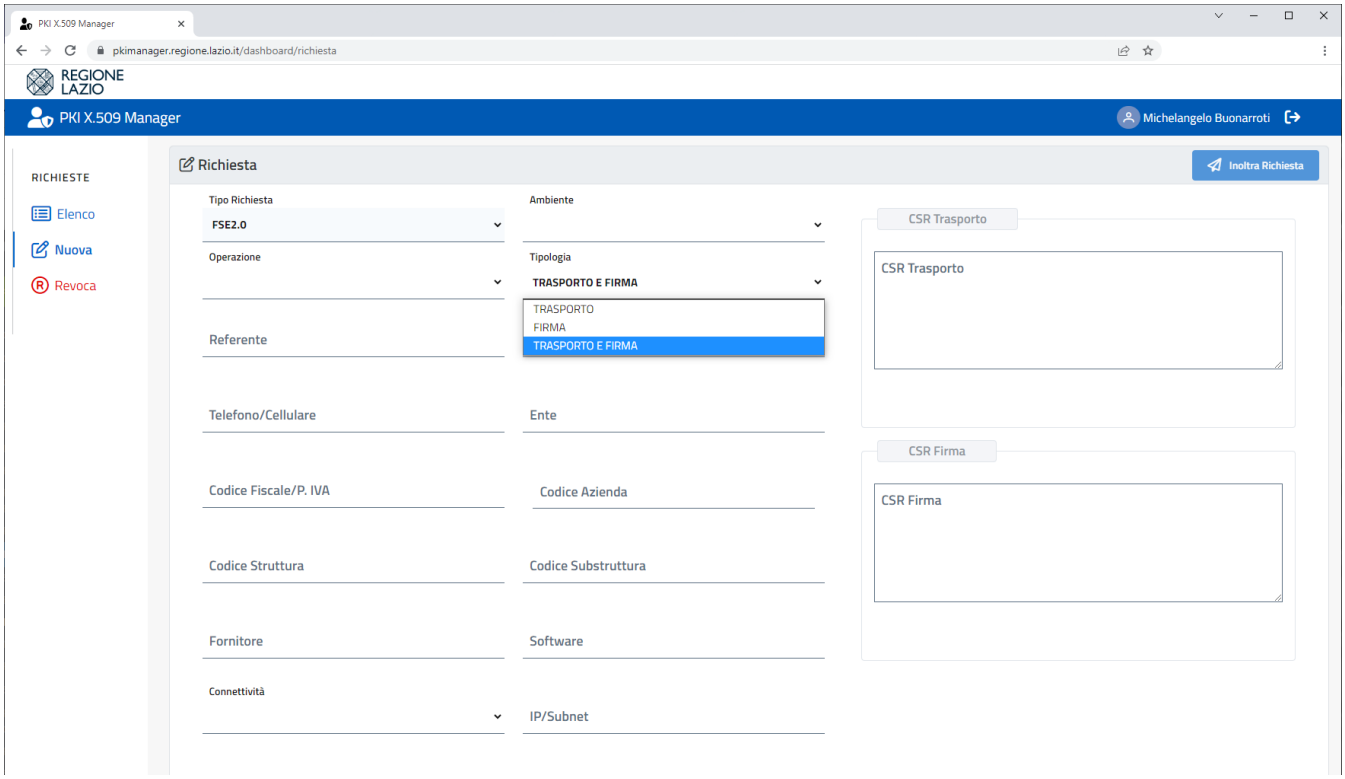
Cliccando su Nuova si aprirà la form di inserimento dati dove ogni campo presente risulta obbligatorio



Per la richiesta dei certificati di Trasporto/Firma saranno necessarie le seguenti informazioni

- Tipologia di operazione: Rilascio | Rinnovo | Revoca
- Ambiente: Produzione | Collaudo
- Tipologia Certificato: Trasporto | Firma | Trasporto + Firma
- Nominativo Referente
- Mail Referente – su tale indirizzo verranno inviati i certificati e tutte le comunicazione relative alle richieste effettuate
- Telefono Cellulare
- Ente – Ragione Sociale
- Codice Fiscale Partita IVA
- Codice Azienda - 6 caratteri di cui solo gli ultimi 3 da valorizzare (le prime 3 cifre sono fisse a 120 per la Regione Lazio) con il codice ministeriale della ASL o AO
- Codice Struttura - 6 cifre che indicano il codice ministeriale della struttura che è presente nei file STS11 o HSP11 in base alla tipologia di erogatore.
  In caso di ASL e A.O. inserire lo stesso codice presente in codice struttura comprensivo delle tre cifre inziali.
- Codice Substruttura – eventuale indicazione della sub struttura all'interno della struttura. Riportare 00 in caso di assenza
- Fornitore
- Software
- Connettività
- IP/Subnet - Indirizzo IP o Subnet dalla quale verranno inviate le richieste di integrazione al fascicolo
- CSR Trasporto / Firma – formato PEM

In relazione al campo “Tipologia” saranno presenti uno o entrambe i box per l’inserimento delle CSR



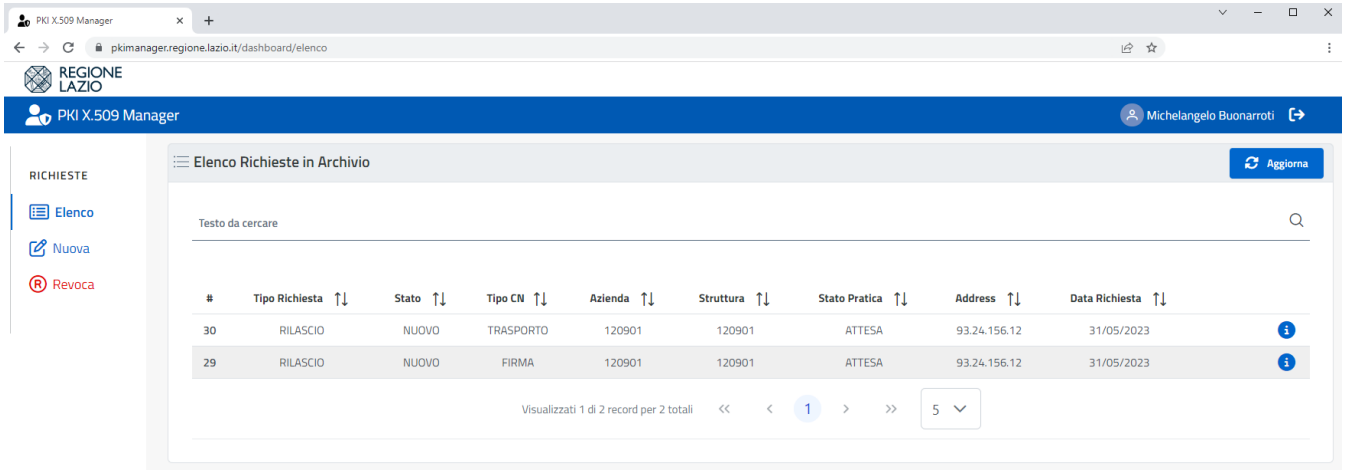
Ogni tipologia di richiesta sarà controllata dal team del Fascicolo Sanitario e solo dopo la loro approvazione verranno generati i certificati ed inviati all’utente indicato.

Compilati correttamente tutti campi il tasto “invia Richiesta” in alto a destra risulterà attivo e sarà possibile concludere il processo di richiesta, il quale dopo un breve messaggio di conferma finalizzerà la richiesta ed invierà alla mail segnala una conferma dell’avvenuto invio.

Nota: in caso di richiesta di entrambe i certificati saranno generate due richieste distinte una per il certificato di Autenticazione e una per quello di firma, conseguentemente arriveranno due email di notifica

Elenco richieste

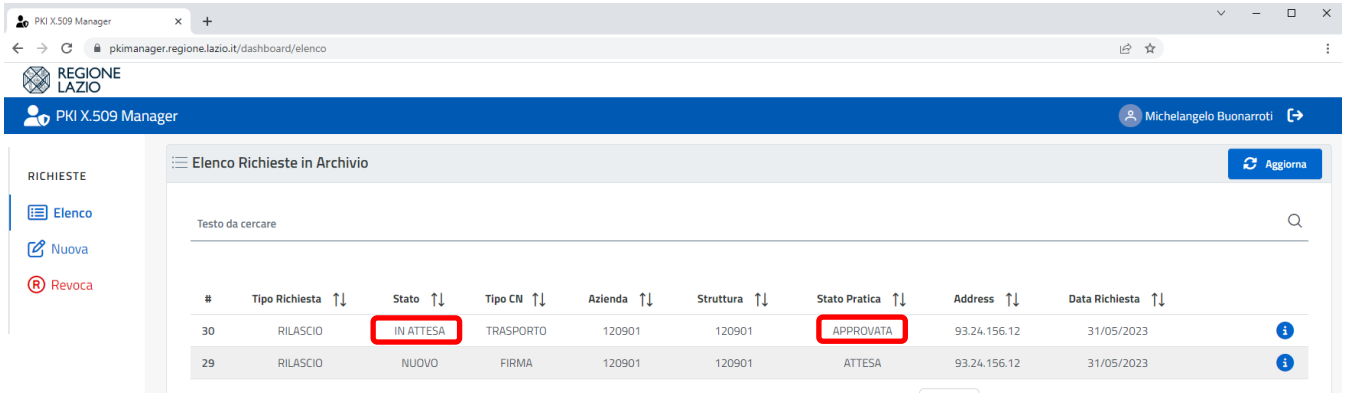
In ogni momento, dal menu contestuale di sinistra cliccando sulla voce Elenco è possibile controllare lo stato delle richieste inserite, vedere il dettaglio, scaricare il certificato, richiederne la revoca



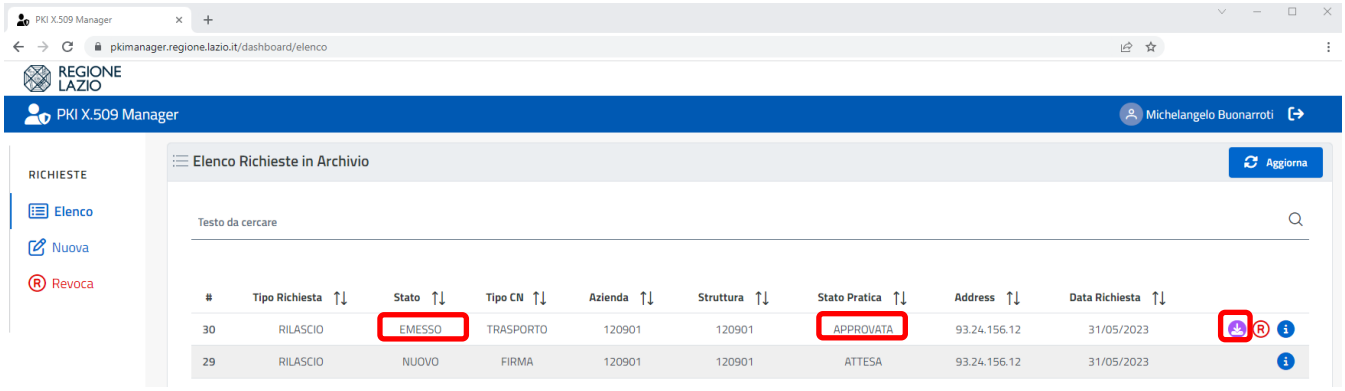
La colonna “Stato” indica lo stato di elaborazione della richiesta di generazione del Certificato.

La colonna “Stato Pratica” indica lo stato di avanzamento della richiesta rispetto al backoffice di controllo

In caso di certificato approvato ed in corso di generazione lo stato apparirà come segue

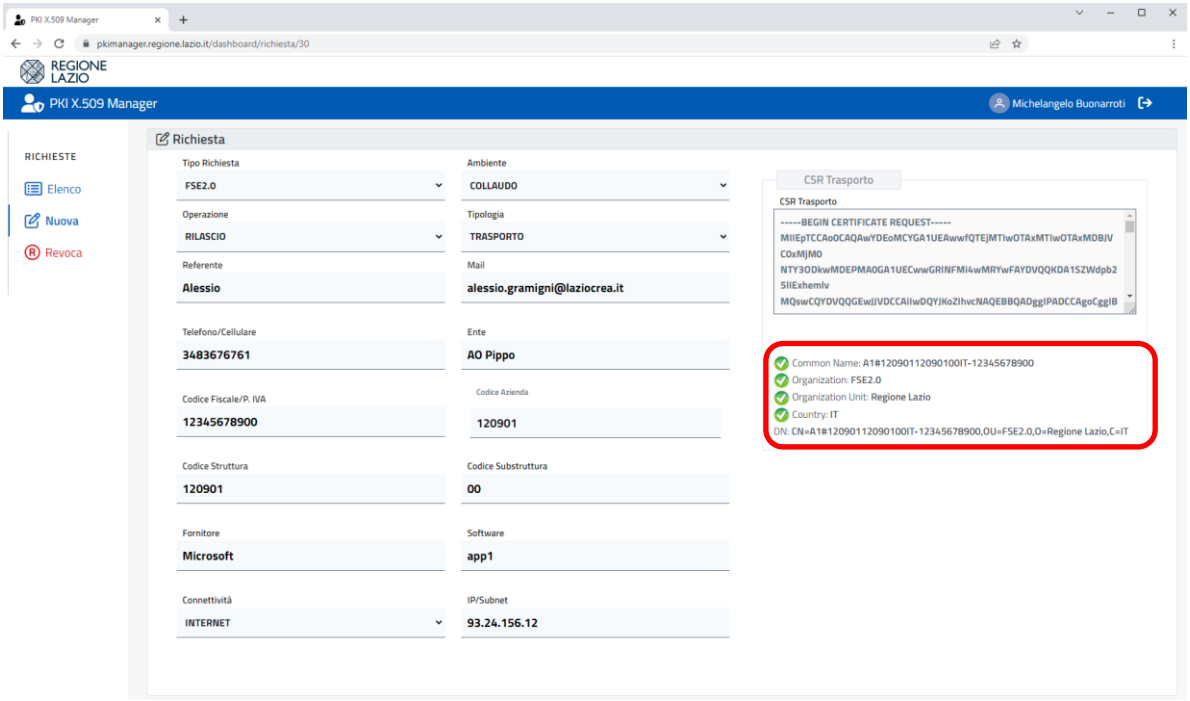


Solo alla fine del processo di generazione sarà possibile scaricare il certificato e vedere la colonna stato aggiornarsi con “Emesso”



Dalla schermata di “Elenco” è anche possibile controllare il dettaglio dei dati inseriti, per tutte le richieste, indipendentemente dal loro stato di avanzamento.

Inoltre è presente una comoda funzionalità che visualizza in chiaro le informazioni che compongono il DN del Certificato

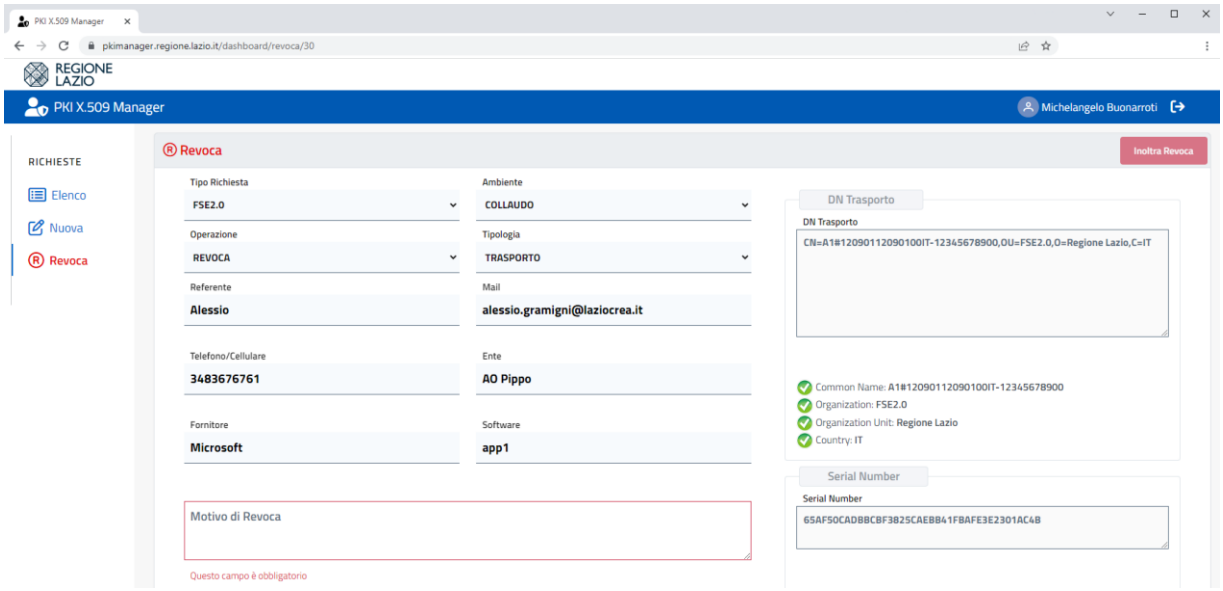


Revoca

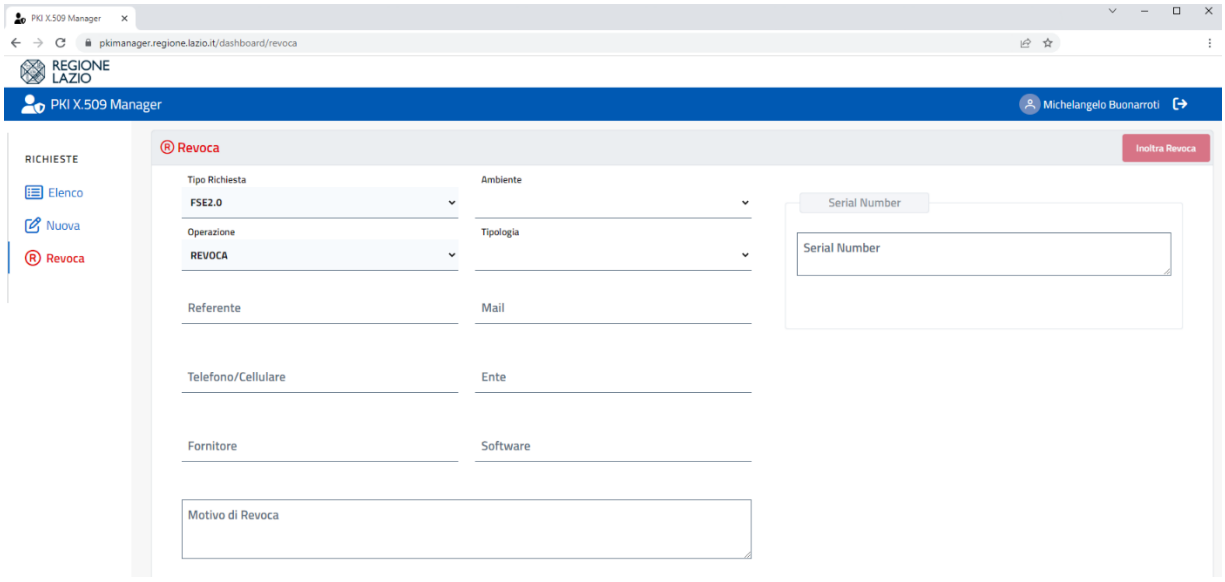
Come descritto in precedenza il processo di revoca di un certificato può essere iniziato

- dal richiedente del certificato originale, mediante l'azione  presente sull'elenco delle richieste
- da un soggetto terzo che conosca il serial number del certificato – mediante il tasto Ⓡ Revoca presente nel menu di sinistra

nel primo caso i campi della revoca saranno già precompilati con quelli presenti nella richiesta originale e dovrà essere solo inserita la motivazione



nel secondo caso invece i campi saranno liberi e andranno <u>tutti</u> compilati manualmente



Per entrambe le casistiche la richiesta dovrà comunque essere vagliata e approvata da un operatore di backoffice che potrà, in caso di non legittimità e/o incongruenza dei dati, rifiutare la richiesta.

Generazione file CSR

Le CSR ovvero Certificate Signing Request sono il file necessari per la corretta emissione dei certificati da parte della PKI di Regione Lazio. I passi fondamentali per la creazione di una CSR sono:

1. Generazione di una chiave privata –almeno 2048 bit, deve rimanare in possesso del solo richiedente e deve essere mantenuta in luogo sicuro
2. Generazione della CSR inserendo i campi fondamentali per la definizione del DN - Distinguished Name
    a. CN: CommonName
    b. OU: OrganizationalUnit
    c. O: Organization
    d. C: CountryName

Al fine di identificare in modo chiaro il richiedente è l'uso che dovrà fare del certificato Regione Lazio ha definito uno standard per la compilazione di tali campi

Distinguished Name (DN) - In caso di certificato di Autenticazione/Trasporto

CN=A1#<<CodiceAzienda>><<CodiceStruttura>><<CodiceSubstruttura>>IT-<<CodiceFiscale>>,O=Regione Lazio,OU=FSE2.0,C=IT

Distinguished Name (DN) – In Caso di Certificato di Firma

CN=S1#<<CodiceAzienda>><<CodiceStruttura>><<CodiceSubstruttura>>IT-<<CodiceFiscale>>_<<Fornitore>>-<<Software>>,O=Regione Lazio,OU=FSE2.0,C=IT

dove:

CodiceAzienda - 6 caratteri di cui solo gli ultimi 3 da valorizzare (le prime 3 cifre sono fisse a 120 per la Regione Lazio) con il codice ministeriale della ASL o AO

CodiceStruttura - 6 cifre che indicano il codice ministeriale della struttura che è presente nei file STS11 o HSP11 in base alla tipologia di erogatore. In caso di ASL e A.O. inserire lo stesso codice presente in codice struttura comprensivo delle tre cifre inziali.

CodiceSubstruttura – eventuale indicazione della sub struttura all'interno della struttura. Riportare 00 in caso di assenza

CodiceFiscale - deve essere popolato con il codice fiscale della persona giuridica a cui il certificato X.509 è associato prefissato da "IT-"

Fornitore – Nominativo del fornitore del software per la gestione della firma senza spazi ne caratteri accentati / speciali

Software – Identificativo del software per la gestione della firma senza spazi ne caratteri accentati / speciali

Esempio di generazione delle CSR mediante openssl

CSR richiesta certificato di Autenticazione / Trasporto

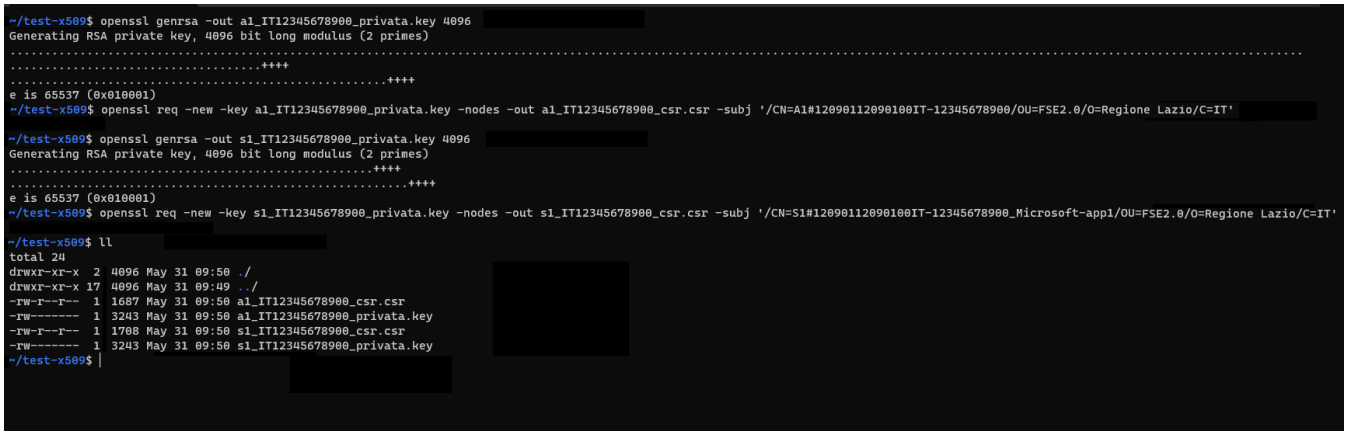
openssl genrsa -out a1_IT12345678900_privata.key 4096

openssl req -new -key a1_IT12345678900_privata.key -nodes -out a1_IT12345678900_csr.csr -subj '/CN=A1#12090112090100IT-12345678900/OU=FSE2.0/O=Regione Lazio/C=IT'

CSR richiesta certificato di Firma

openssl genrsa -out s1_IT12345678900_privata.key 4096

openssl req -new -key s1_IT12345678900_privata.key -nodes -out s1_IT12345678900_csr.csr -subj '/CN=S1#12090112090100IT-12345678900_Microsoft-app1/OU=FSE2.0/O=Regione Lazio/C=IT'



Per controllare il contenuto delle CSR e la corretta compilazione del DN

openssl req -in a1_IT12345678900_csr.csr -noout -text

openssl req -in s1_IT12345678900_csr.csr -noout -text

```
~/test-x509$ openssl req -in a1_IT12345678900_csr.csr -noout -text
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: CN = A1#12090112090100IT-12345678900, OU = FSE2.0, O = Regione Lazio, C = IT
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
```

```
~/test-x509$ openssl req -in s1_IT12345678900_csr.csr -noout -text
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: CN = S1#12090112090100IT-12345678900_Microsoft-app1, OU = FSE2.0, O = Regione
Lazio, C = IT
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
```