Emissione certificato

Emissione - Introduzione

La Certification Authority permette di rilasciare un certificato di firma remota ad un titolare in modo che lui/lei possa usarlo per firmare digitalmente dei documenti.

Clienti

Un certificato è rilasciato ad un titolare **E** all'interno di un bucket cliente. Quindi un certificato è sempre associato ad un titolare **E** al cliente.

Tipi di certificato

Possono essere rilasciati 4 differenti tipologie di certificato:

- **AUTO**: è la tipologia di certificato utilizzato per le procedure di 'backoffice' in cui si firmano massivamente un elevato numero di documenti senza l'interazione del titolare. Di solito ha un limite d'uso.
- **SEAL**: è come **AUTO** ma per 'soggetti giuridici'.
- **FEQ**: è un certificato senza limiti d'uso che può essere usato solo con procedure aggiuntive di strong auth e per firmare un numero limitato di documenti per sessione di firma.
- **ONESHOT**: è come **FEQ** ma ha dei limiti molto stringenti di durata e/o numero di firme apponibili.

Identificazione

Per rilasciare un certificato, è importante identificare il futuro titolare.

Un certificato può essere rilasciato **dopo** o **prima** dell'identificazione:

- se un certificato è rilasciato dopo, parliamo di un processo di identificazione **ex-ante**
- al contrario di un processo di identificazione **ex-post**

Nel flusso **ex-post** il certificato viene rilasciato attivo ma sospeso e la Certification Authority attende che l'identificazione produca i dovuti documenti per riattivarlo.

Con le API correnti un certificato può essere rilasciato secondo i seguenti flussi:

- **Ex-ante and direct**: significa che il titolare deve essere identificato prima di richiedere il certificato e tutti i dati necessari al rilascio devono essere forniti all'API di emissione(ex. PIN ove necessario).

Procedure di identificazione

Le API correnti gestiscono 3 tipi di identificazione:

- **SPID**: tramite SPID
- **CIE**: tramite CIE
- **FEQ**: tramite una firma digitale valida
- **VIDEO**: tramite una piattaforma VIDEO di 3e parti

Modalità di identificazione e documenti da caricare

Come detto la Certification Authority accetta 3 modalità di identificazione:

- FEQ
- SPID
- CIE
- VIDEO

SPID

nel caso di identificazione SPID, dovranno essere forniti due documenti:

- la saml request
- la saml response

prodotte dall'identificazione SPID. Ovviamente dovranno essere documenti:

1. validi
2. con firma integra
3. relativi al titolare per il quale si sta facendo la richiesta
4. non scaduti

ATTENZIONE: per definizione lo SPID richiede che la persona da identificare sia in possesso di un codice fiscale italiano. In caso contrario l'emissione del certificato verrà bloccata.

CIE

nel caso di identificazione CIE, dovranno essere forniti due documenti:

- la saml request
- la saml response

prodotte dall'identificazione CIE. Ovviamente dovranno essere documenti:

1. validi
2. con firma integra
3. relativi al titolare per il quale si sta facendo la richiesta
4. non scaduti

ATTENZIONE: per definizione lo CIE richiede che la persona da identificare sia in possesso di un codice fiscale italiano. In caso contrario l'emissione del certificato verrà bloccata.

VIDEO

nel caso di identificazione VIDEO le API non richiedono alcun documento. O meglio, si aspettano che arrivi in seconda battuta uno zip contenente tutto ciò che la piattaforma di video riconoscimento ha prodotto.

FEQ

nel caso di identificazione FEQ dovrà essere fornito il pdf del modulo di richiesta opportunamente firmato dal titolare nei campi firma previsti con un certificato valido

EVIDENZE

inoltre le API richiedono, con l'eccezione del caso in cui si parli di identificazione FEQ, le evidenze che il titolare abbia accettato o meno le clausole riportate sul modulo di richiesta, di cui deve prendere obbligatoriamente visione.
Le evidenze hanno la seguente struttura:

```
{
    "owner#clause#signature#1":  true,
    "owner#clause#signature#2": true,
    "owner#clause#signature#3": true,
    "owner#clauses#1#yes": true,
    "owner#clauses#2#yes": false
}
```

Emissione - API ex-ante/direct

ex-ante/direct vuol dire, come già detto, che occorre fornire in fase di emissione tutte le info relative all'identificazione del titolare e tutti i dati necessari per emettere il certificato.

Chiamata di apertura richiesta di certificato

Per aprire una richiesta di certificato occorre chiamare il servizio:

> Apertura richiesta ex-ante

Nella chiamata occorre passare diverse informazioni:


```
{
  "profile": "string",
  "rao": {
    "certificateAlias": "string",
    "alias": "string"
  },
  "organization": {
    "name": "string",
    "unit": "string",
    "identifier": "string",
    "country": "string",
    "city": "string",
    "district": "string",
    "cap": "string",
    "address": "string",
    "email": "string",
    "processApplication": "string",
    "responsibleDocument": "string",
    "responsiblePosition": "string"
  },
  "owner": {
```

```
    "alias": "string",
    "firstName": "string",
    "lastName": "string",
    "sex": "string",
    "birthCity": "string",
    "birthCountry": "string",
    "birthDate": "2023-07-02",
    "birthDistrict": "string",
    "city": "string",
    "country": "string",
    "district": "string",
    "cap": "string",
    "address": "string",
    "email": "string",
    "phoneNumber": "string",
    "pec": "string",
    "fiscalCode": "string",
    "document": {
      "issuer": "string",
      "country": "string",
      "number": "string",
      "releaseDate": "2023-07-02",
      "expiryDate": "2023-07-02",
      "type": "IDC"
    }
  }
}
```

- **profile** è il nome del profilo di emissione. Contiene tutte le informazioni relative al tipo di certificato, all'identificazione richiesta, alla durata, alle possibili modalità di identificazione, al fatto che richieda o meno un pin etc...
- **rao** è il Registration Authority Officer, cioè la persona che si assume la responsabilità di emettere il certificato. Normalmente è un rappresentate del cliente. E' necessario fornire il suo alias(identificativo), mentre l'alias del certificato è opzionale. Ha senso solo se il RAO ha più di un certificato associato.
- **owner** è il titolare del certificato
- **organization** è l'organizzazione (azienda) per la quale il titolare lavora/opera. Obbligatorio nel caso di emissione di sigilli.

Il servizio esegue una validazione molto stringente dei valori forniti:

nome	obbligatorio	regex	condizioni	dipendenze
owner.firstName	x	[\w\s]{1,128}		
owner.lastName	x	[\w\s]{1,128}		
owner.sex	x	[FMfm]{1}		
owner.birthCity	x	ricavato dal servizio messo a disposizione dalla CA		
owner.birthCountry	x	iso alpha 2		
owner.birthdate	x	yyyy-MM-dd	>=18 && <=120 anni	
owner.birthDistrict	x	ricavato dal servizio messo a disposizione dalla CA		
owner.city	x	ricavato dal servizio messo a disposizione dalla CA		
owner.country	x	iso alpha 2		
owner.district	x	ricavato dal servizio messo a disposizione dalla CA		
owner.cap	x	[0-9]{3,10}		
owner.address	x	[\w\s]{1,128}		
owner.email	x	si applica reg exp relativa alla mail		
owner.pec		si applica reg exp relativa alla mail		
owner.phone	x	[+0-9]{8,15}		
owner.fiscalNumber		codice fiscale valido e ricavabile dai valori precedenti		
document.issuer	x	[\w\s]{1,128}		
document.country	x	iso alpha 2		
document.number	x	si applica reg exp relative al numero di documento		

document.releaseDate	x	yyyy-MM-dd	<=oggi	
document.expiryDate	x	yyyy-MM-dd	>oggi	
document.type	x	IDC|PAS|DLC		Se fiscalNumber non fornito il type potrà essere solo PAS
organization.name	x	[\w\s]{1,128}		obbligatorio solo per certificati di tipo SEAL
organization.unit		[\w\s]{1,128}		
organization.identifier	x	[\w\s]{1,128}		obbligatorio solo per certificati di tipo SEAL
organization.country	x	iso alpha 2		obbligatorio solo per certificati di tipo SEAL
organization.city	x	ricavato dal servizio messo a disposizione dalla CA		obbligatorio solo per certificati di tipo SEAL
organization.district	x	ricavato dal servizio messo a disposizione dalla CA		obbligatorio solo per certificati di tipo SEAL
organization.cap	x	[0-9]{3,10}		obbligatorio solo per certificati di tipo SEAL
organization.address	x	[\w\s]{1,128}		obbligatorio solo per certificati di tipo SEAL
organization.email	x	si applica reg exp relativa alla mail		obbligatorio solo per certificati di tipo SEAL
organization.processApplication	x	[\w\s]{1,128}		obbligatorio solo per certificati di tipo SEAL
organization.responsibleDocument		[\w\s]{1,128}		
organization.responsiblePosition		[\w\s]{1,128}		

Chiamata di completamento richiesta di certificato

Per completare una richiesta di certificato occorre chiamare il servizio:

> Completamento richiesta ex-ante

Il servizio può essere invocato solo con un token TSID di tipo API dello stesso cliente che ha aperto la richiesta.

Nella chiamata occorre passare diverse informazioni:

```
{
    "rao": {
        "certificatePin": "12345678"
    },
    "identificationProcess":"VIDEO",
    "identificationDocs": {

    },
    "extra": {
        "pin": "12345678"
    },
    "webhook": {
        "url": "callback_url"
    }
}
```

- **rao.certificatePin** è pin del certificato del RAO utilizzato per emettere il certificato
- **identificationProcess** indica il processo di identificazione utilizzato. E' un campo opzionale poichè nel caso di profili con un singolo processo associato questa informazione è ininfluente
- **extra.pin** è pin che si vuole associare al certificato che si sta emettendo. Ammesso che il certificato necessiti di un pin.
- **webhook.url** è l'url del webhook che il servizio invocherà per comunicare l'esito dell'operazione. Infatti il servizio in questione è asincrono.
- **identificationDocs** è la sezione che contiene i documenti di identificazione del titolare. Esistono due modi per fornire i documenti e si rimanda alla sezione relativa

Il servizio, in quanto, asincrono, ritorna un **202** per segnalare la presa in carico dell'operazione.

Ad emissione completata, il servizio avrà cura di:

- inviare al titolare (e se SEAL anche alla mail di organization) una mail con le indicazioni relative al certificato emesso, con in allegato il pdf del modulo di richiesta opportunamente firmato sia dal titolare che dal RAO
- inviare un webhook all'integratore con i dati del certificato
- inviare tutti i documenti prodotti in conservazione

Reg exp numero documento, in base al type

- IDC: ^([a-zA-Z]{2}[ ]?[\d]{5}[ ]?[a-zA-Z]{2}|[a-zA-Z]{2}[ ]?[\d]{7})$
- PAS: ^[a-zA-Z]{2}[\d]{7}$
- DLC: ^[U]1[A-Za-z0-9]{8}$ **OR** ^[A-Z]{2}\d{7}[A-Z]$

Reg exp mail

Data la mail user@domain

- user: (^[-!#$%&'+/=?^_`{}|~0-9A-Z]+(\.[-!#$%&'*+/=?^_`{}|~0-9A-Z]+)\Z|^"([\001-\010\013\014\016-\037!#-\[\]-\177]|\\[\001-\011\013\014\016-\177])*"\Z)
- domain: (?:A-Z0-9?\.)+(?:[A-Z]{2,6}|[A-Z0-9-]{2,}(?<!-))\Z

In risposta il servizio ritorna:

```
{
  "requestId": "64a0895e8620872ba1be33e7",
  "document":
"JVBERi0xLjYNJeLjz9MNCjQ5NiAwIG9iag0.......2SBV65FF6ic7HWtBZlDsR5T5FuYsFKZgHdlWwD/Rc8BLt/wGjSc
ohDQplbmRzdHJlYW0KZW5kb2JqCnN0YXJ0eHJlZgoyNzg1NTMKJSVFT0YK"
}
```

dove:

- **requestId** è l'id della richiesta appena aperta
- **document** è il pdf del modulo di richiesta opportunamente fillato in base 64. Tale modulo deve essere preso in visione dal
  titolare

Modalità di caricamento dei documenti di identificazione

In fase di chiamata di completamento

La modalità più semplice è rappresentata dal passaggio dei documenti in fase di chiamata di completamento all'interno del campo **identificationDocs**:

SPID

```
"identificationDocs": {
  "documents": [
    {
      "name": "evidences.json",
```

```
      "data":
"JVBERi0xLjYNJeLjz9MNCjQ5NiAwIG9iag08PC9MaW5lYXJpemVkIDEvTCAyNTA1NDQvTyA0OTgvRSAyMTAwNDkvTiAzL
1QgMjUwMTE2L0ggWyA3NzEgNDQ5XT4+DWVuZG9iag0gICAgICAgICAgICAgICAgDQo1NjIgMCBvYmoNPDwvRGVjb2RlUGFybXM
8PC9Db2x1bW5zIDUvUHJlZGljdG9yIDEyPj4vRmlsdGVyL0ZsYXRlRGVjb2RlL0lEWzwxM0VEQkU4Rjg5NjQ5NjRBODYyN
TcwOUIxMEQ1REJFRD48RkIxMTM4OUE0OTI1OEI0Mzg5QUYyNDYzRUY0QUUxRT....."
    },
    {
      "name" : "spid.request.xml",
      "data" :
"JVBERi0xLjYNJeLjz9MNCjQ5NiAwIG9iag08PC9MaW5lYXJpemVkIDEvTCAyNTA1NDQvTyA0OTgvRSAyMTAwNDkvTiAzL
1QgMjUwMTE2L0ggWyA3NzEgNDQ5XT4+DWVuZG9iag0gICAgICAgICAgICAgICAgDQo1NjIgMCBvYmoNPDwvRGVjb2RlUGFybXM
8PC9Db2x1bW5zIDUvUHJlZGljdG9yIDEyPj4vRmlsdGVyL0ZsYXRlRGVjb2RlL0lEWzwxM0VEQkU4Rjg5NjQ5NjRBODYyN
TcwOUIxMEQ1REJFRD48RkIxMTM4OUE0OTI1OEI0Mzg5QUYyNDYzRUY0QUUxRT....."
    },
    {
      "name" : "spid.response.xml",
      "data" :
"JVBERi0xLjYNJeLjz9MNCjQ5NiAwIG9iag08PC9MaW5lYXJpemVkIDEvTCAyNTA1NDQvTyA0OTgvRSAyMTAwNDkvTiAzL
1QgMjUwMTE2L0ggWyA3NzEgNDQ5XT4+DWVuZG9iag0gICAgICAgICAgICAgICAgDQo1NjIgMCBvYmoNPDwvRGVjb2RlUGFybXM
8PC9Db2x1bW5zIDUvUHJlZGljdG9yIDEyPj4vRmlsdGVyL0ZsYXRlRGVjb2RlL0lEWzwxM0VEQkU4Rjg5NjQ5NjRBODYyN
TcwOUIxMEQ1REJFRD48RkIxMTM4OUE0OTI1OEI0Mzg5QUYyNDYzRUY0QUUxRT....."
    }
  ]
}
```


CIE


```
"identificationDocs": {
  "documents": [
    {
      "name": "evidences.json",
      "data":
"JVBERi0xLjYNJeLjz9MNCjQ5NiAwIG9iag08PC9MaW5lYXJpemVkIDEvTCAyNTA1NDQvTyA0OTgvRSAyMTAwNDkvTiAzL
1QgMjUwMTE2L0ggWyA3NzEgNDQ5XT4+DWVuZG9iag0gICAgICAgICAgICAgICAgDQo1NjIgMCBvYmoNPDwvRGVjb2RlUGFybXM
8PC9Db2x1bW5zIDUvUHJlZGljdG9yIDEyPj4vRmlsdGVyL0ZsYXRlRGVjb2RlL0lEWzwxM0VEQkU4Rjg5NjQ5NjRBODYyN
TcwOUIxMEQ1REJFRD48RkIxMTM4OUE0OTI1OEI0Mzg5QUYyNDYzRUY0QUUxRT....."
    },
    {
      "name" : "cie.request.xml",
      "data" :
```

```
"JVBERi0xLjYNJeLjz9MNCjQ5NiAwIG9iag08PC9MaW5lYXJpemVkIDEvTCAyNTA1NDQvTyA0OTgvRSAyMTAwNDkvTiAzL
1QgMjUwMTE2L0ggWyA3NzEgNDQ5XT4+DWVuZG9iag0gICAgICAgICAgICAgICAgDQo1NjIgMCBvYmoNPDwvRGVjb2RlUGFybXM
8PC9Db2x1bW5zIDUvUHJlZGljdG9yIDEyPj4vRmlsdGVyL0ZsYXRlRGVjb2RlL0lEWzwxM0VEQkU4Rjg5NjQ5NjRBODYyN
TcwOUIxMEQ1REJFRD48RkIxMTM4OUE0OTI1OEI0Mzg5QUYyNDYzRUY0QUUxRT....."
    },
    {
      "name" : "cie.response.xml",
      "data" :
"JVBERi0xLjYNJeLjz9MNCjQ5NiAwIG9iag08PC9MaW5lYXJpemVkIDEvTCAyNTA1NDQvTyA0OTgvRSAyMTAwNDkvTiAzL
1QgMjUwMTE2L0ggWyA3NzEgNDQ5XT4+DWVuZG9iag0gICAgICAgICAgICAgICAgDQo1NjIgMCBvYmoNPDwvRGVjb2RlUGFybXM
8PC9Db2x1bW5zIDUvUHJlZGljdG9yIDEyPj4vRmlsdGVyL0ZsYXRlRGVjb2RlL0lEWzwxM0VEQkU4Rjg5NjQ5NjRBODYyN
TcwOUIxMEQ1REJFRD48RkIxMTM4OUE0OTI1OEI0Mzg5QUYyNDYzRUY0QUUxRT...."
    }
  ]
}
```


VIDEO


```
"identificationDocs": {
  "documents": [
    {
      "name": "evidences.json",
      "data":
"JVBERi0xLjYNJeLjz9MNCjQ5NiAwIG9iag08PC9MaW5lYXJpemVkIDEvTCAyNTA1NDQvTyA0OTgvRSAyMTAwNDkvTiAzL
1QgMjUwMTE2L0ggWyA3NzEgNDQ5XT4+DWVuZG9iag0gICAgICAgICAgICAgICAgDQo1NjIgMCBvYmoNPDwvRGVjb2RlUGFybXM
8PC9Db2x1bW5zIDUvUHJlZGljdG9yIDEyPj4vRmlsdGVyL0ZsYXRlRGVjb2RlL0lEWzwxM0VEQkU4Rjg5NjQ5NjRBODYyN
TcwOUIxMEQ1REJFRD48RkIxMTM4OUE0OTI1OEI0Mzg5QUYyNDYzRUY0QUUxRT...."
    }
  ]
}
```


FEQ


```
"identificationDocs": {
  "documents": [
    {
      "name": "request_module.pdf",
      "data":
"JVBERi0xLjYNJeLjz9MNCjQ5NiAwIG9iag08PC9MaW5lYXJpemVkIDEvTCAyNTA1NDQvTyA0OTgvRSAyMTAwNDkvTiAzL
1QgMjUwMTE2L0ggWyA3NzEgNDQ5XT4+DWVuZG9iag0gICAgICAgICAgICAgICAgDQo1NjIgMCBvYmoNPDwvRGVjb2RlUGFybXM
```

```
8PC9Db2x1bW5zIDUvUHJlZGljdG9yIDEyPj4vRmlsdGVyL0ZsYXRlRGVjb2RlL0lEWzwxM0VEQkU4Rjg5NjQ5NjRBODYyN
TcwOUIxMEQ1REJFRD48RkIxMTM4OUE0OTI1OEI0Mzg5QUYyNDYzRUY0QUUxRT...."
    }
  ]
}
```


Con chiamata separata

Un'altra possibilità è rappresentata dal servizio di caricamento:

> Caricamento documenti

Tale metodo ritorna in output una stringa **storageFolder** che indica il bucket dove i documenti sono stati caricati.

Quindi, in fase di chiamata di completamento, sarà sufficiente andare a fornire tale info all'interno di **identificationDocs**:

```
"identificationDocs": {
  "storageFolder": "nome"
}
```

Esempio di webhook finale con le informazioni di emissione


```
{
  "success": true,
  "traceId": "bc45872a9bb9c0c554b72b0c63a08686",
  "id": "651a7b31a1dbc2080aa58b67",
  "context": "CERTIFICATE_CREATION",
  "event": "EMITTED",
  "data": {
    "certificate": {
      "alias": "70724",
      "validFrom": "2023-10-02T08:11:00",
      "validTo": "2024-10-01T14:11:00",
      "profile": "AUTO",
      "signaturesNumber": 0
    },
    "owner": {
      "alias": "TINIT-FRMTTR76M06B715E",
      "firstName": "Ettore",
```

```
      "lastName": "Fieramosca",
      "birthDate": "1976-08-06",
      "birthDistrict": "CE",
      "birthCity": "Capua",
      "birthCountry": "IT",
      "sex": "M",
      "email": "a.mariano@teamsystem.com",
      "phoneNumber": "+393452495944"
    }
  }
}
```


I webhook emessi dal servizio saranno tutti caratterizzati dal context **CERTIFICATE_CREATION.** Il valore del campo **EVENT** permetterà di distinguere la tipologia di evento.

EMITTED per esempio sarà il valore del campo evento che segnalerà il completamento dell'emissione del certificato