MANUALE OPERATIVO

GoNotice

QERDS PRACTICE STATEMENT

CODICE DOCUMENTO	ICERT-QERDS-MO
VERSIONE 1.2	
DATA	11/11/2024

INFOCERT
TINEXTA GROUP

Sommario

1 INTRODUZIONE

1.1 Novità introdotte rispetto alla precedente emissione

Informazione	Dettaglio
Versione/Release n°:	**1.2**
Data Versione/Release:	**10/11/2024**
Descrizione modifiche:	**Aggiornamenti paragrafi 3.3.2, 3.5.1, 3.5.2**
Motivazioni:	**Chiarimenti**

Informazione	Dettaglio
Versione/Release n°:	**1.1**
Data Versione/Release:	**18/10/2024**
Descrizione modifiche:	• **Correzione errori** • **Revisione formattazione del documento** • **Miglioramento della struttura ai fini dell'accessibilità del documento** • **Revisione delle definizioni e degli acronimi** • **Revisione dei riferimenti normativi, procedurali e tecnici** • **Aggiornamento sede legale** • **Aggiornamento dei soggetti responsabili dell'approvazione del Manuale Operativo** • **Revisione e omologazione della nomenclatura dei i ruoli del servizio e specificazione delle loro caratteristiche** • **Semplificazione della descrizione dei processi**
Motivazioni:	**Revisione generale del documento**

Informazione	Dettaglio
Versione/Release n°:	**1.0**
Data Versione/Release:	**05/06/2024**
Descrizione modifiche:	**Prima emissione del documento**
Motivazioni:	**-**

1.2 Quadro generale

Il presente documento è il Manuale Operativo del Prestatore di Servizi Fiduciari InfoCert (*Trust Service Provider*) che descrive il servizio **GoNotice**, **servizio elettronico di recapito certificato qualificato.**

Il servizio GoNotice è realizzato nel rispetto del Regolamento UE N. 910/2014 eIDAS 0..

Il manuale contiene le politiche e le pratiche seguite nel processo di identificazione e rilascio del servizio GoNotice, le misure di sicurezza adottate, gli obblighi, le garanzie e le responsabilità, in conformità con la vigente normativa in materia di servizi fiduciari qualificati.

Pubblicando tale Manuale Operativo e inserendo i riferimenti a tale documento nella contrattualistica e in appositi link delle interfacce d'uso, si consente agli utenti di valutare le

caratteristiche e l'affidabilità del servizio GoNotice offerto da InfoCert, e quindi le modalità di accesso al servizio nonché del legame ed i rapporti che intercorrono tra servizio stesso e *Cliente*.

Il presente Manuale Operativo contiene altresì le **politiche e le pratiche** seguite da InfoCert nel processo di controllo delle richieste, identificazione del *Responsabile* in base al *Contratto* (cfr. paragrafo §1.3.4) e nel **rilascio del servizio** di cui all'art. 3, def. 37) e art. 44 del Regolamento UE N. 910/2014 eIDAS [1], **sulla base del Testo Unico del Codice dell'Amministrazione Digitale** (**CAD**) [2] **e delle disposizioni di AGID** sulle modalità per la presentazione delle domande di iscrizione nella Trusted List come ERDSP (Electronic Registered Delivery Service Provider), ed **in conformità con** i requisiti e **policy di sicurezza** definite nello standard ETSI EN 319 521 [6] .

Il **servizio di recapito certificato qualificato,** specificato nel presente Manuale Operativo, è contraddistinto da una serie di caratteristiche che sono pienamente identificate e connesse, nei paragrafi che seguono, agli standard e ai regolamenti (o specifiche parti di essi) che ne rappresentano la base di supporto.

Si riportano qui di seguito gli aspetti essenziali di più alto livello che sono poi ulteriormente dettagliati nelle successive specifiche sezioni.

Il principale tratto che contraddistingue il servizio GoNotice è quello di essere definito in accordo alle **policy e security requirements** definite nello standard ETSI EN 319 521[6]. In altre parole, dal punto di vista più generale possibile, si tratta di un servizio che in tale standard è definito come **Electronic Registered Delivery Service (ERDS)**.

Un flusso di GoNoice, dal punto di vista generale e in assenza di ambiguità, può essere identificato dal cosiddetto *style of operation* denominato "**Store and Notify**" (**S&N** da qui in avanti): il messaggio del mittente viene sottoposto al servizio per essere inviato, il servizio lo memorizza (**store**) in delle aree dedicate al cliente mittente ed invia al destinatario una notifica (**notify**) con quanto necessario perché il ricevente possa accedere al messaggio del mittente.

1.3 Identificazione del documento

1.3.1 Nome ed identificativo del documento

Questo documento è denominato "InfoCert - Prestatore di Servizi di Recapito Certificato qualificato – Manuale Operativo GoNotice" (*QERDS Practice Statement*) ed è caratterizzato dal codice documento: ICERT-QERDS-MO. La versione e il livello di rilascio sono identificabili nell'intestazione di ogni pagina.

Al documento sono associati gli Object Identifier (OID) (cfr. def. paragrafo §1.3.4) e gli Uniform Resource Identifier (URI), descritti in seguito.

L'*object identifier* (OID) che identifica **InfoCert** è **1.3.76.36**.

Lo *Uniform Resource Identifier* (URI) radice, che identifica degli oggetti significativi nell'ambito degli standard ETSI, è **http://uri.etsi.org** (o https://uri.etsi.org).

Gli identificativi significativi per servizio di recapito certificato qualificato e per il relativo

Manuale Operativo sono:

Descrizione	OID
Servizio recapito certificato qualificato	1.3.76.36.1.1.2000
Manuale-operativo-servizio-recapito-certificato qualificato	1.3.76.36.1.1.2000.1

Tabella 1 – Identificativi

1.3.2 Scopo e campo di applicazione del documento

Il presente documento ha lo scopo di descrivere le regole e le procedure operative adottate da InfoCert nella conduzione del servizio di **servizio di recapito certificato qualificato** in accordo alle norme e standard correnti, come riportato al paragrafo §1.2.

Il presente manuale costituisce, inoltre, un'integrazione di dettaglio all'informativa fornita al *Cliente* ai sensi dell'articolo 13 del D.Lgs. 196/03 e l'art. 13 del Regolamento (UE) 679/2016 [3].

1.3.3 Riferimenti normativi e tecnici

1.3.3.1 Riferimenti normativi e tecnici

[1] **Regolamento UE N. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014** in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE modificato dal Regolamento UE N. 2024/1183 del Parlamento Europeo e del Consiglio dell'11 aprile 2024 (referenziato come EIDAS)

[2] **Decreto Legislativo 7 marzo 2005, n.82** (G.U. n.112 del 16 maggio 2005 - S.O. n. 93) – Codice dell'amministrazione digitale (referenziato anche come CAD) e ss.m.ii.

[3] **Decreto Legislativo 30 giugno 2003, n. 196** (G.U. n. 174 del 29 luglio 2003) – Codice Privacy e ss.mm.ii e Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (vigente dal 25 maggio 2018).

[4] **Direttiva 2011/83/UE del Parlamento europeo e del Consiglio, del 25 ottobre 2011**, sui diritti dei consumatori e relative normative nazionali di recepimento.

[5] **ETSI EN 319 401** "Electronic Signatures and Infrastructures (ESI): General Policy Requirements for Trust Service Providers".

[6] **ETSI EN 319 521** "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers".

[7] **ETSI EN 319 522** "Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services"

[8] **Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013** (GU Serie Generale n.117 del 21-05-2013) – "Regole tecniche in materia di generazione, apposizione e verifica delle

firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71".

[9] **ETSI EN 319 403** "Requirements for conformity assessment bodies assessing Trust Service Providers".

[10] **IETF RFC 6749** "The OAuth 2.0 Authorization Framework"

[11] **IETF RFC 6750** "The OAuth 2.0 Authorization Framework: Bearer Token Usage"

1.3.3.2 Standard di riferimento procedurali

Tutti i processi operativi del QERDSP InfoCert descritti in questo Manuale Operativo, come ogni altra attività del QERDSP InfoCert, sono svolti in modalità conforme al Piano di qualità aziendale e di sicurezza, in accordo agli standard **UNI EN ISO/IEC 9001:2015** e **UNI CEI EN ISO/IEC 27001:2013**.

1.3.3.3 Standard di riferimento di sicurezza

Per assicurare la sicurezza del servizio di recapito certificato qualificato, InfoCert utilizza tecniche e procedure basate su standard (de jure o de facto) internazionali e sulle norme specifiche esistenti in Italia.

Nella redazione e nella messa a punto delle procedure ci si è basati sugli standard:

- **Information Technology Security Evaluation Criteria (ITSEC) v. 1.2**
- **Common Criteria for Information Technology Security Evaluation v 2.2**
- **ISO/IEC 17799** - Information technology -- Security techniques -- Code of practice for information security management
- **UNI CEI EN ISO/IEC 27001:2013** - Sicurezza delle informazioni, cybersecurity e protezione della privacy - Sistemi di gestione per la sicurezza delle informazioni – Requisiti UNI CEI ISO/IEC 27001:06 – Tecnologia delle Informazioni – Tecniche di Sicurezza – Sistemi di gestione della sicurezza delle informazioni – Requisiti.
- **ISO IEC 27002:05** – Information Technology – Security Techniques – Code of practice for Information Security Management
- **UNI CEI EN ISO/IEC 27017** - Tecnologie Informatiche - Tecniche di sicurezza - Raccolta di prassi sui controlli per la sicurezza delle informazioni per i servizi in cloud basata sulla ISO/IEC 27002
- **UNI CEI EN ISO/IEC 27018** - Tecnologie informatiche - Tecniche di sicurezza - Raccolta di prassi per la protezione dei dati personali trattati in cloud pubblici da responsabili del trattamento
- **UNI CEI ISO/IEC 29115** - Tecnologie informatiche - Tecniche per la sicurezza - Quadro di riferimento per la garanzia dell'autenticazione delle entità

I moduli crittografici (HSM) utilizzati da InfoCert per le chiavi di firma digitale dei contenuti e delle evidenze (ERDS evidence) sono validati e certificati FIPS 140-2 level 3 e Common Criteria (CC) Information Technology Security Evaluation Assurance Level (EAL).

1.3.4 Definizioni

Sono di seguito elencate le definizioni utilizzate nella stesura del presente documento. Per i termini definiti nelle norme sopra referenziate si rimanda alle definizioni in essi stabilite.

Termine	Definizione
Cliente	**Persona fisica o giuridica che acquista/richiede il servizio di recapito certificato qualificato e si assume la facoltà di sospenderlo o revocarlo.**
Titolare	Persona fisica o giuridica, richiedente il servizio,che dovrà essere identificata come Titolare del servizio del recapito certificato qualificato. **Il Titolare è il soggetto mittente (*Sender*) di tutte le comunicazioni effettuate nell'utilizzo del servizio. In alcuni casi il Titolare coincide con il cliente.**
Responsabile	Persona fisica che verrà effettivamente identificata in quanto Titolare (persona fisica) o legale rappresentante del Titolare o persona munita di procura del Titolare
Intermediario	Con il termine *Intermediario autorizzato* (o semplicemente *Intermediario*) si intende il partner commerciale (o distributore) di InfoCert che svolge attività a supporto della rete di vendita diretta del servizio GoNotice attraverso un apposito contratto di rivendita.
Utente	Persona o applicazione autorizzata ad accedere al servizio GoNotice tramite autenticazione.
Utente-Admin	Utente che accede al servizio GoNotice attraverso le credenziali del servizio di recapito certificato qualificato che si occupa di censire nuove utenze.
Utente-Sender	Utente che accede al servizio GoNotice attraverso le credenziali del servizio di recapito certificato qualificato che si occupa dell'invio dei messaggi certificati.
Mittente / Sender	Il Titolare che invia la comunicazione al destinatario.
Destinatario / Receiver	Persona fisica che riceve la comunicazione da parte del mittente a seguito di identificazione.
Identity Provider (IdP)	Gestore dell'identità digitale.
Servizio elettronico di recapito certificato (SERC)	«Servizio che consente la trasmissione di dati fra terzi per via elettronica e fornisce prove relative al trattamento dei dati trasmessi, fra cui prove dell'avvenuto invio e dell'avvenuta ricezione dei dati, e protegge i dati trasmessi dal rischio di perdita, furto, danni o di modifiche non autorizzate» (cfr art, 3, def.36) eIDAS [1]).
Electronic registered delivery service (ERDS)	Come definito all'articolo 3 del Regolamento eIDAS[1] « a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations; » (cfr art, 3, def.36) eIDAS [1]).
Servizio elettronico di	Servizio elettronico di recapito certificato che soddisfa i seguenti requisiti:

Termine	Definizione
recapito certificato qualificato (SERCQ)/ Qualified Electronic Registered Delivery Service (QERDS)	a) sono forniti da uno o più prestatori di servizi fiduciari qualificati; b) garantiscono con un elevato livello di sicurezza l'identificazione del mittente; c) garantiscono l'identificazione del destinatario prima della trasmissione dei dati; d) l'invio e la ricezione dei dati sono garantiti da una firma elettronica avanzata o da un sigillo elettronico avanzato di un prestatore di servizi fiduciari qualificato in modo da escludere la possibilità di modifiche non rilevabili dei dati; e) qualsiasi modifica ai dati necessaria al fine di inviarli o riceverli è chiaramente indicata al mittente e al destinatario dei dati stessi; f) la data e l'ora di invio e di ricezione e qualsiasi modifica dei dati sono indicate da una validazione temporale elettronica qualificata.» (cfr art, 3, def.37) e art.44 eIDAS [1]). Ove non espressamente indicato, nel presente documento, per "servizio" si intende "servizio di recapito certificato qualificato".
Servizio GoNotice	Il **Servizio elettronico di recapito certificato qualificato erogato da InfoCert**.
Autorità per la marcatura temporale / Time-stamping authority	Prestatore di servizi qualificato, che agisce da terza parte fidata, che eroga il servizio di marcatura temporale {Time-stamping authority}.
Organismo di valutazione della conformità/ Conformity Assessment Body (CAB)	Organismo accreditato a norma del Regolamento eIDAS come competente a effettuare la valutazione della conformità del prestatore di servizi fiduciari qualificato e dei servizi fiduciari qualificati da esso prestati. Redige il CAR. (cfr. art.3 def. 18) eIDAS [1]).
Relazione di valutazione della conformità / Conformity Assessment Report (CAR)	Relazione con cui l'organismo di valutazione della conformità conferma che il prestatore di servizi fiduciari qualificati e i servizi fiduciari stessi rispettano i requisiti del Regolamento (cfr. artt.21 e 51 eIDAS [1]).
Open ID Connect & OAuth2.0	Protocollo di autenticazione interoperabile basato sul quadro di specifiche oAuth 2.0 (IETF RFC 6749 [10] e 6750[11]). Semplifica il modo di verificare l'identità degli utenti in base all'autenticazione eseguita da un server di autorizzazione e permette di ottenere informazioni sul profilo utente in modo interoperabile e simile al modello REST.TitolareOAuth
Livello di Garanzia / Level of Assurance (LoA)	Livello di sicurezza o di garanzia dei regimi di identificazione elettronica progressivamente crescente in base alla sensibilità del servizio erogato. Sono individuati tre livelli di garanzia (cfr. art. 8 comma2 eIDAS [1]) in base a quanto definito dallo standard ISO/IEC 29115: • livello 1- Basso/Low (corrispondente al LoA2 dell'ISO-IEC 29115): • livello 2 – Medio/Substantial (corrispondente al LoA3 dell'ISO-IEC 29115); • livello 3 – Alto/High (corrispondente al LoA4 dell'ISO-IEC 29115). Per il dettaglio di rimanda alla norma ISO. Il livello minimo di garanzia permesso per autenticazione e riconoscimento del mittente è il livello 2 .
Contratto	Il contratto per l'attivazione del servizio di recapito certificato qualificato GoNotice è composto dalla Richiesta di Attivazione, dalle Condizioni Generali di Contratto, da questo Manuale Operativo e dai documenti ivi richiamati che costituiscono complessivamente la disciplina dei rapporti tra le parti.

Termine	Definizione
Credenziali dell'Utente	Insieme di dati e fattori propri di un *Utente* utilizzati per accedere al servizio di recapito certificato qualificato attraverso un sistema di autenticazione a due fattori. Titolare
Dati di identificazione personale	Un insieme di dati che consente di stabilire l'identità di una persona fisica o giuridica, o di una persona fisica che rappresenta una persona giuridica (cfr. eIDAS [1]).
Identificazione elettronica	Il processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica o giuridica, o un'unica persona fisica che rappresenta una persona giuridica (cfr. eIDAS [1]).
Marca temporale	Il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo (cfr. art.1, def, h) DPCM 22 febbraio 2013)[8].
Mezzi di identificazione elettronica	Un'unità materiale e/o immateriale contenente dati di identificazione personale e utilizzata per l'autenticazione per un servizio online (cfr. eIDAS [1]).
Password usata una sola volta / One Time Password (OTP)	Password valida solo per una singola transazione. Nell'ambito del servizio di recapito certificato qualificato può essere utilizzata come *secondo fattore di autenticazione* a convalida delle *Credenziali dell'Utente.*
Prestatore di servizi fiduciari qualificato	Un prestatore di servizi fiduciari che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato (cfr. eIDAS [1]).
Richiesta di attivazione	La richiesta del *Titolare* in cui viene richiesta l'attivazione del servizio di recapito certificato qualificato GoNotice.

Tabella 2 - Definizioni

1.3.5 Acronimi e abbreviazioni

Acronimo	Definizione
AgID	**Agenzia per l'Italia Digitale: autorità di Vigilanza sui Prestatori di Servizi Fiduciari**
CA	**Certification Authority**
CAB	**Conformity Assessment Body – Organismo di valutazione della conformità**
CAD	**Codice dell'Amministrazione Digitale (cfr. DL 7 Marzo 2005 0)**
CAR	**Conformity Assessment Report – Relazione di valutazione della conformità**
CIE	**Carta di Identità Elettronica**
eID	**Electronic Identity**
eIDAS	**Electronic Identification and Signature Regulation (cfr. 0)**
ETSI	**European Telecommunications Standards Institute**
HTTPS	**HyperText Transfer Protocol Secure**
IP (o Indirizzo IP)	**Indirizzo numerico che identifica gli elaboratori connessi alla rete.**
ISO	**International Organization for Standardization: fondata nel 1946, l'ISO è un'organizzazione internazionale costituita da organismi nazionali per la standardizzazione**
OID	**Object Identifier: è costituito da una sequenza di numeri, registrata secondo la procedura indicata nello standard ISO/IEC 6523, che identifica un determinato oggetto all'interno di una gerarchia**
SPID	**Sistema Pubblico di Identità Digitale**
S&N	**Store and Notify**

Tabella 3 – Acronimi e abbreviazioni

1.4 Manuale Operativo

Il presente Manuale Operativo, compilato dal QERDS InfoCert nel rispetto delle disposizioni generali degli standard di riferimento (ETSI EN 319 521 [6]), è fornito all'organismo di vigilanza designato - che per l'Italia è AGID - ed è parte costituente la documentazione di qualificazione di prestatore di servizio di recapito certificato qualificato.

1.4.1 Periodo e meccanismo di notifica

Il Manuale Operativo è pubblicato:

- in formato elettronico sul sito Web del QERDS InfoCert (indirizzo: http://www.infocert.it/documentazione);
- in formato elettronico nell'elenco pubblico dei certificatori tenuto da AgID;
- in formato cartaceo può essere richiesto all'*Intermediario autorizzato* o al contatto per gli utenti finali.

1.4.2 Soggetti responsabili dell'approvazione del Manuale Operativo

Questo Manuale Operativo viene verificato dal Responsabile della Sicurezza e delle Policy, dal Responsabile della Privacy, dal Responsabile del Servizio di Certificazione, dal Responsabile Legale, dal Responsabile Regulatory e approvato dalla Direzione Aziendale.

1.4.3 Procedure di approvazione

La redazione e approvazione del manuale seguono le procedure previste dal Sistema di Gestione per la Qualità dell'Azienda ISO 9001:2015.

Con frequenza non superiore all'anno, il Prestatore di Servizi Fiduciari esegue un controllo di conformità di questo Manuale Operativo al proprio processo di erogazione del servizio di certificazione.

1.4.4 Revisione del Manuale Operativo

InfoCert si riserva di apportare variazioni al presente documento per esigenze tecniche o per modifiche alle procedure intervenute sia a causa di norme di legge o regolamenti, sia per ottimizzazioni del ciclo lavorativo.

Ogni nuova versione del Manuale Operativo annulla e sostituisce le precedenti versioni.

Variazioni che non hanno un impatto significativo sugli utenti comportano l'incremento del numero di release del documento, mentre variazioni con un impatto significativo sugli utenti (come, ad esempio, modifiche rilevanti alle procedure operative) comportano l'incremento del numero di versione del documento. In ogni caso il manuale sarà prontamente pubblicato e reso disponibile.

Con frequenza non superiore all'anno, il QERDS InfoCert esegue un controllo di conformità di questo Manuale Operativo al proprio processo di erogazione del servizio di recapito certificato qualificato.

2 RUOLI DEL SERVIZIO GONOTICE

2.1 Fornitore del servizio GoNotice

Il servizio di recapito certificato qualificato GoNotice consente di trasmettere contenuti, fornendo prove relative al trattamento del messaggio trasmesso, fra cui l'avvenuto invio, e

protegge i messaggi trasmessi dal rischio di perdita, furto, danni o di modifiche non autorizzate.

In questo documento, quando non diversamente specificato, si usa il termine QERDS per indicare QERDS Service Provider InfoCert.

I dati completi dell'organizzazione che svolge la funzione di **QERDS** sono i seguenti:

Denominazione sociale	**InfoCert – Società per azioni** **Società soggetta a direzione e coordinamento di Tinexta S.p.A.**
Sede legale	**Piazzale Flaminio 1/B, 00196 – Roma**
Sedi operative	**Piazzale Flaminio 1/B, 00196 – Roma** **Via Fernanda Wittgens n. 2, 20123 Milano (MI)** **Piazza Luigi da Porto n. 3, 35131 Padova (PD)**
Rappresentante legale	**Danilo Cattaneo - In qualità di Amministratore Delegato**
N. di telefono	**06 836691**
Partita IVA/Codice Fiscale	**07945211006**
N. Iscr. Registro Imprese	**Business Register N. 07945211006 -** *N. REA* **RM - 1064345**
Sito Web	**https://www.infocert.it**

2.2 Intermediario autorizzato

Il servizio viene commercializzato da InfoCert sia attraverso rete di vendita diretta, sia tramite partner indicati all'interno del presente documento sotto il nome di **Intermediario autorizzato** - come definito al paragrafo al paragrafo §1.3.4

L'intermediario ha come unico compito quello di rivendere il servizio erogato da InfoCert.

2.3 Cliente

La presente persona o soggetto giuridico è definita al paragrafo §1.3.4.

2.4 Titolare

La presente persona o soggetto giuridico è definita al paragrafo §1.3.4.

2.5 Responsabile

La presente persona o soggetto giuridico è definita al paragrafo §1.3.4.

2.6 Utente-Admin e Utente-Sender

La persona all'interno della organizzazione del Titolare a cui è demandata la gestione del servizio (Utente-Admin) e l'invio delle comunicazioni (Utente-Admin o Utente-Sender) è definita al paragrafo § 1.3.41.3.4.

2.7 Mittente

Titolare che invia la comunicazione al destinatario, come definito al paragrafo §1.3.4.

2.8 Destinatario

La persona che riceve la comunicazione dal mittente, come definita al paragrafo §1.3.4.

3 IDENTIFICAZIONE E AUTENTICAZIONE

3.1 Generalità sulle procedure per l'identificazione

I paragrafi di questo capitolo descrivono le procedure usate per l' identificazione del *Titolare* necessaria all'attivazione del servizio di recapito certificato qualificato GoNotice.

La procedura di identificazione comporta che il *Titolare* sia riconosciuto da InfoCert, che ne verificherà l'identità attraverso una delle modalità definite nei successivi paragrafi del presente capitolo.

3.2 Identificazione del Titolare persona fisica o giuridica

La richiesta del servizio di recapito certificato qualificato per un **Titolare persona fisica** verrà effettata attraverso la procedura descritta al paragrafo successivo.

La richiesta del servizio di recapito certificato qualificato per un **Titolare persona giuridica** (organizzazione) deve essere effettuata da una persona fisica, il *Responsabile*, identificata nello stesso modo del Titolare persona fisica, in una delle modalità descritte al paragrafo successivo.

Il Responsabile, inoltre, deve presentare la documentazione relativa alla persona giuridica e la documentazione o procura, che attesti il titolo ad avanzare la richiesta per conto della persona giuridica.

3.2.1 Identificazione tramite firma elettronica qualificata

Per l'attivazione del servizio GoNotice è necessario che il Titolare compili e firmi digitalmente il modulo di richiesta di attivazione del servizio che dovrà compilare con le seguenti informazioni:

- dati del Titolare del servizio di recapito certificato qualificato
- dati del Responsabile (se Titolare persona fisica è coincidente con il Titolare)
- dati della persona incaricata a svolgere le funzioni di utente "Admin" *(*cfr. paragrafo §1.3.4)
- accettazione delle condizioni generali del servizio
- riferimento (identificativo mail) della persona della struttura tecnica interna all'organizzazione Titolare che seguirà le fasi operative di attivazione del servizio.

3.3 Processo di verifica e attivazione del servizio

3.3.1 Processo di verifica della richiesta

Infocert, attraverso il proprio personale opportunamente formato, avvia il processo di verifica per procedere poi all'attivazione del servizio.

Le verifiche effettuate per permettere l'attivazione sono le seguenti:

- verifica della validità della firma del Richiedente
- nel caso il Titolare sia una entità giuridica, InfoCert, verifica che il richiedente abbia poteri di firma
- eventuale verifica della procura in caso il richiedente non sia il legale rappresentante.

Il controllo, la supervisione e l'aggiornamento delle procedure necessarie alla verifica dei poteri di firma e delle eventuali verifiche relative alla procura sono effettuati da InfoCert sotto sua responsabilità.

3.3.2 Attivazione del servizio

Terminate le verifiche, l'attivazione procede con la seguente modalità.

InfoCert prende contatto con la struttura tecnica (indicata dal Titolare nel modulo di attivazione) per la raccolta delle informazioni relative al sistema di autenticazione e autorizzazione.

Il Titolare del servizio deve indicare le informazioni necessarie per poter abilitare un accesso sicuro almeno di livello 2 (*medio/substantial - LoA3 dell'ISO-IEC 29115*).

Per l'accesso al servizio è necessario che InfoCert configuri opportunamente il sistema oAuth 2.0 dedicato all'organizzazione cliente, impostando, tramite console Web:

- il nuovo Titolare, con le informazioni relative
- il sistema di autenticazione del Titolare, come da specifiche della struttura tecnica
- l'Utente-Admin, come indicato nel modulo di attivazione

e informi il Titolare della avvenuta configurazione.

Dopo l'attivazione, l'Utente-Admin potrà accedere all'interfaccia Web di GoNotice (cfr. paragrafo §4.3.1) con le proprie credenziali, definite dall'organizzazione nell'ambito del proprio sistema di autenticazione, e da essa opportunamente profilate. Il sistema di autenticazione deve essere almeno di livello 2 (*medio/substantial - LoA3 dell'ISO-IEC 29115*).

3.4 Sistema oAuth 2.0 per l'autenticazione

Per l'autenticazione degli utenti (*Utente-Admin e all'Utente-Sender*), GoNotice utilizza OpenID Connect (OIDC).

OpenID Connect (OIDC) è un protocollo di autenticazione basato su oAuth 2.0, uno standard ampiamente adottato, che permette alle applicazioni di autenticare gli utenti verificando

l'identità attraverso un Identity Provider (IdP) compatibile con OIDC, come ad esempio Google, Microsoft Azure, o un IdP aziendale.

Applicando un'autenticazione forte, con almeno un livello 2 (*medio/substantial - LoA3 dell'ISO-IEC 29115*) OIDC garantisce che gli account del mittente aderiscano a protocolli di autenticazione avanzati (Multi-Factor Authentication - MFA) per una maggiore sicurezza. Ciò è particolarmente importante data la natura sensibile delle comunicazioni gestite da GoNotice.InfoCert richiede, pertanto, che l'organizzazione Titolare del servizio, sia provvista di un servizio di autenticazione e autorizzazione con protocollo oAuth (*i sistemi più utilizzati sono Microsoft Authenticator e Google Authenticator*) e che l'autenticazione debba essere almeno di livello 2 (*medio/substantial - LoA3 dell'ISO-IEC 29115*).

La responsabilità della verifica dell'identità degli utenti è pertanto delegata al servizio di autenticazione e autorizzazione utilizzato dal Titolare.

InfoCert ha la facoltà di non accettare sistemi di autenticazione ritenuti non idonei all'utilizzo di GoNotice.

3.4.1 Profili utente del servizio

Il servizio GoNotice prevede due profili: l'Utente-Admin e l'Utente-Sender.

3.4.1.1 Utente-Admin

La persona, che accede al servizio GoNotice attraverso le credenziali del servizio di recapito certificato qualificato, a cui è demandata, all'interno dell'organizzazione del Titolare, la gestione del servizio.

In particolare, l'Utente-Admin si occupa di censire nuove utenze (di tipo Utente-Admin e Utente-Sender) (cfr. paragrafo §1.3.4).

Il profilo abilitato solo nell'interfaccia Web.

3.4.1.2 Utente-Sender

Utente che accede al servizio GoNotice attraverso le credenziali del servizio di recapito certificato qualificato e si occupa dell'invio dei messaggi certificati (cfr. paragrafo §1.3.4).il profilo abilitato nell'interfaccia Web e in API.

3.5 Credenziali applicative per accesso API

Oltre alla modalità manuale tramite interfaccia Web, il servizio di recapito certificato qualificato permette di avere una API di accesso per le funzioni di invio e verifica, che possono essere integrate dal Titolare in modalità applicativa.

In questo scenario un'applicazione del Titolare può collegarsi al servizio e schedulare in modo automatizzato gli invii, effettuare verifiche sullo stato dei recapiti, integrare processi del cliente con invii certificati all'interno del servizio.

Per l'integrazione applicativa InfoCert rilascia credenziali oAuth 2.0 che il Titolare può portare

nelle applicazioni per l'autenticazione API.

L'interfaccia API mette a disposizione le funzioni descritte al paragrafo §4.5.2.

3.5.1 Rilascio delle credenziali API

Per il rilascio delle credenziali applicative, il Titolare:

- effettua richiesta a InfoCert, indicando un identificativo per distinguere l'applicazione/processo del cliente che utilizzerà tali credenziali
- InfoCert predispone e fornisce le credenziali di accesso in modalità sicura al Titolare.

Nella richiesta è possibile indicare la durata delle credenziali, comunque non oltre i 15 minuti, per permettere al Titolare di limitare l'accesso al solo tempo necessario all'applicazione/processo che ne deve fare uso.

Il servizio, nell'utilizzo dell'interfaccia API, tiene traccia nei log delle operazioni effettuate dalle applicazioni, con identificazione delle credenziali utilizzate.

Il Titolare deve concordare con InfoCert le modalità di rilascio e distribuzione delle credenziali sul proprio sistema di autenticazione che dovrà rispettare almeno di livello 2 (*medio/substantial - LoA3 dell'ISO-IEC 29115*).

3.5.2 Sospensione o revoca delle credenziali API

Il Titolare, in qualsiasi momento, può sospendere o revocare le credenziali API.

Questa operazione permette di bloccare, nella fase di autenticazione, l'accesso al servizio.

Per procedere alla sospensione/revoca delle credenziali API, il Titolare richiede a InfoCert

InfoCert

1. verifica autenticità della richiesta
2. sospende/revoca l'utenza e credenziali
3. avvisa il Titolare della rimozione.

In seguito alla sospensione/revoca non verrà più permesso l'accesso al servizio.

4 FUNZIONALITÀ DEL SISTEMA

4.1 Generalità

Il servizio di recapito certificato qualificato **GoNotice**, gestito ed erogato da InfoCert, permette ad un mittente di inviare delle comunicazioni certificate qualificate ad uno o più destinatari, nel paradigma *Store and Notify*.

Il contenuto della comunicazione, che può contenere anche allegati, viene preso in carico dal servizio e propagato al destinatario, secondo le modalità operative descritte in questo capitolo.

Sia il mittente che il destinatario vengono identificati nella transazione di invio della comunicazione. Tutte le operazioni effettuate dal mittente e dal destinatario vengono tracciate e gestite in modo sicuro dal servizio.

Il servizio non permette alcuna modifica del contenuto originale una volta inviato.

I paragrafi che seguono descrivono nel dettaglio le modalità operative di utilizzo.

4.2 Modalità di utilizzo del servizio

Il servizio di recapito certificato qualificato GoNotice prevede due modalità per l'utilizzo del servizio.

4.2.1 Interfaccia Web

In questo caso gli utenti possono utilizzare le varie funzionalità previste dal servizio in modalità manuale.

4.2.2 Interfaccia API

Tramite API, un'interfaccia applicativa esposta per l'integrazione da parte di applicazioni del Titolare, il servizio GoNotice può essere utilizzato dai processi gestiti dal cliente.

4.3 Accesso al servizio

4.3.1 Accesso tramite interfaccia Web

Dopo l'attivazione, gli utenti (*Utente-Admin* e *Utente-Sender*) possono accedere all'interfaccia Web con le proprie credenziali, definite dall'organizzazione nell'ambito del proprio sistema di autenticazione, e da essa opportunamente profilate.

L'accesso all'interfaccia Web di GoNotice prevede l'autenticazione di livello 2 (*medio/substantial - LoA3 dell'ISO-IEC 29115*).

Ad ogni accesso è necessario effettuare una nuova autenticazione.

Anche al destinatario (*Receiver*) viene richiesto di identificarsi, tramite autenticazione SPID di livello 2 (*medio/substantial - LoA3 dell'ISO-IEC 29115*) o CIE, per poter accedere al contenuto a lui destinato.

Una volta autenticato al servizio (cfr. capitolo §3), l'utente può accedere all'interfaccia Web ed utilizzare le funzionalità del sistema fino alla scadenza della sessione o al logout esplicito dell'utente.

4.3.2 Accesso tramite API

L'accesso tramite API viene protetto tramite protocollo oAuth 2.0, con credenziali rilasciate al Titolare (vedi procedure descritte al § 3.5), che permettono di autenticare l'applicazione chiamante del Titolare.

4.3.3 Sessione e protocolli di trasmissione

La sessione, sia nell'interfaccia Web sia in API, scade in modo automatico dopo 1 ora di inattività.

L'accesso, sia tramite interfaccia Web sia tramite API, prevede l'utilizzo di protocollo HTTPS TLS versione 1.2 o 1.3, garantendo l'autenticazione del server in modo sicuro, la protezione del dato nella fase di invio del mittente (interfaccia Web o API) e l'accesso ai contenuti del *destinatario*/*Receiver* (interfaccia Web).

4.4 Gestione delle utenze

L'interfaccia Web di GoNotice consente all'Utente-Admin di gestire le utenze già presenti nel proprio Identity Provider (IdP).

La gestione dei profili consente agli amministratori di gestire e mantenere il controllo sull'accesso al sistema, garantendo che solo gli utenti autorizzati possano utilizzare GoNotice.

Attraverso l'interfaccia Web, l'Utente-Admin può registrare nuove utenze (di tipo *Utente-Admin* e *Utente-Sender*) e assegnare ruoli e permessi specifici agli utenti all'interno del servizio.

Nello specifico, l'Utente-Admin è infatti autonomo, nel poter:

- abilitare e gestire nuovi Utente-Admin per la gestione del servizio
- abilitare e gestire nuovi Utente-Sender per predisporre ed effettuare nuovi invii.

Gli utenti, Utente-Admin e Utente-Sender, devono far parte dell'organizzazione del Titolare, e, pertanto, devono essere censiti nel sistema di autenticazione configurato.

Una volta registrate le utenze, l'autenticazione delle stesse viene delegata al sistema di autenticazione del Titolare tramite il protocollo oAuth 2.

Nel caso in cui si desideri revocare l'accesso di una di queste utenze al servizio GoNotice, l'Utente-Admin può cancellarla dall'interfaccia. In questo modo, l'utenza non potrà più accedere a GoNotice.

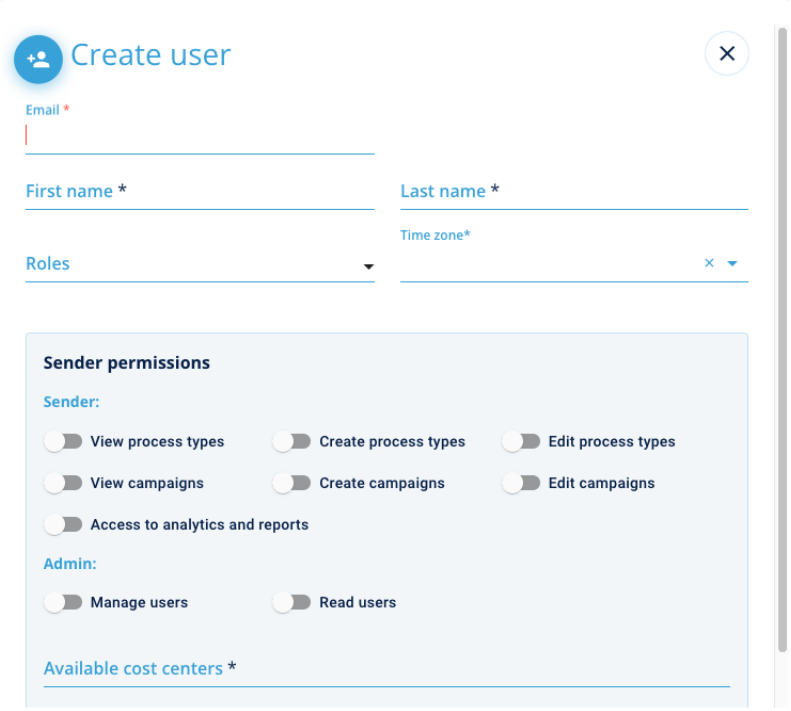

Figura 1- Schermata di creazione utenza

Per creare un nuovo Utente-Sender, l'utente-Admin deve inserire l'email aziendale registrata sul IdP della propria azienda, assegnare un ruolo appropriato e configurare il centro di costo a cui l'Utente-Sender apparterrà.

I privilegi previsti per i profili sono i seguenti:

- Utente-Admin:
  - Manage users: *creare/cancellare e gestire le utenze assegnando il centro di costo su cui gli utenti hanno visibilità*
  - Read users: *visualizzare le utenze censite sulla piattaforma*.
- Utente-Sender:
  - View process types: *visionare la lista dei tipi di processo già creata*
  - Create process types: *creare nuovi tipi di processo*
  - Edit process types: *abilitare l'utente-sender a cambiare i tipi di processo*
  - View campaigns: *visionare le campagne create*
  - Create campaings: *creare nuove campagne*
  - Edit campagins: *modificare campagne esistenti*
  - Access to analytics and reports: *accedere alla Dashboard delle comunicazioni*

4.5 Invio delle comunicazioni

Per l'invio delle comunicazioni, il Titolare può scegliere il metodo più adatto alle proprie esigenze e preferenze:

- tramite interfaccia Web
- tramite una interfaccia applicativa API

4.5.1 Invio tramite interfaccia Web

L'interfaccia di GoNotice offre una piattaforma per la configurazione e l'invio delle comunicazioni.

Una volta effettuato l'accesso al sistema (cfr. paragrafo §4.3), l'utente (*Utente-Admin* e *Utente-Sender*) accede a un'interfaccia che fornisce gli strumenti necessari per poter creare un processo di creazione della comunicazione.

La prima fase consiste nella definizione dei dettagli fondamentali, come il titolo della comunicazione, la lista dei destinatari e il contenuto del messaggio. Qui, il mittente ha la possibilità di personalizzare il testo, aggiungere allegati e selezionare il canale di invio preferito tra le opzioni disponibili, come email, SMS o WhatsApp.

Una volta definiti tutti i parametri necessari (Figura 2), il mittente può visualizzare un'anteprima della comunicazione per verificare che tutto sia corretto e completo.

GoNotice offre anche altre funzionalità, come la programmazione dell'invio in un momento specifico nel futuro e la creazione di modelli predefiniti per semplificare il processo di configurazione delle comunicazioni ricorrenti.

Dopo aver confermato i dettagli, il mittente può inviare la comunicazione. Una volta inviato, GoNotice monitora attentamente lo stato della comunicazione, fornendo aggiornamenti in tempo reale sulle consegne, le aperture e le interazioni dei destinatari. Questa visibilità completa consente al mittente di tracciare l'efficacia della comunicazione.

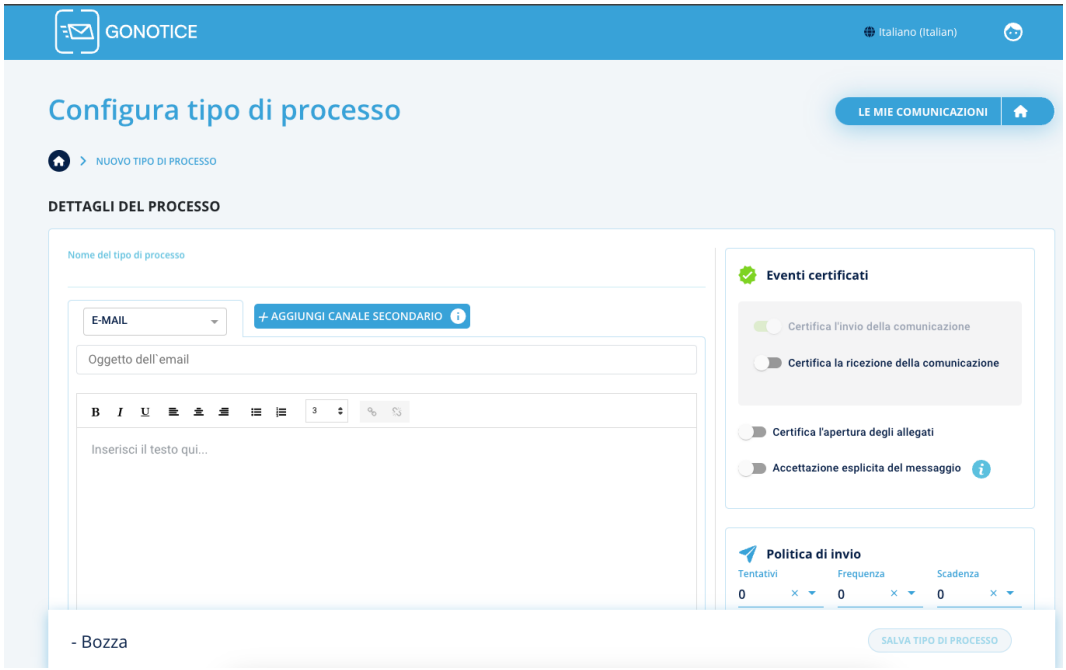

Figura 2 - Schermata di configurazione di un processo

4.5.2 API di accesso al servizio

GoNotice offre API pubbliche che consentono agli sviluppatori di integrare facilmente le funzionalità della piattaforma nei propri sistemi e applicazioni. L'accesso a queste API è gestito

tramite oAuth 2 (cfr. paragrafo §4.3.2).

OAuth 2 fornisce una serie di caratteristiche che lo rendono ideale per l'integrazione delle API di GoNotice. Tra queste caratteristiche vi sono la gestione sicura delle credenziali degli utenti, la delega delle autorizzazioni tramite token di accesso, la separazione dei ruoli e delle autorizzazioni e la scalabilità per supportare un grande numero di utenti e applicazioni.

Per semplificare ulteriormente il processo di integrazione delle API di GoNotice, è disponibile un DevPortal online. Questa piattaforma fornisce agli sviluppatori un accesso centralizzato a documentazione dettagliata, esempi di codice, specifiche di Swagger e altre risorse utili per comprendere e utilizzare le API di GoNotice in modo efficace. Attraverso il DevPortal, gli sviluppatori possono accedere a istruzioni dettagliate su come autenticarsi, eseguire le richieste API e utilizzare tutte le funzionalità offerte dal prodotto.

4.6 Modalità di gestione del contenuto

Il servizio di recapito certificato qualificato GoNotice prevede che il contenuto dell'invio, con relativi allegati, non venga inviato al destinatario attraverso i canali di comunicazione, bensì:

- il contenuto da mettere a disposizione del destinatario viene preso in carico da servizio e viene mantenuto in modo protetto e sicuro all'interno del servizio
- viene predisposto un URL unico per permettere al destinatario di accedere al contenuto tramite il servizio
- viene inoltrato al destinatario l'URL tramite il canale di comunicazione scelto dal mittente.

Il destinatario non può quindi accedere al contenuto prima di aver effettuato le fasi di accesso al servizio ed identificazione, come previsto dalle specifiche QERDS.

4.7 Canali per l'invio

GoNotice offre una varietà di canali per l'invio delle comunicazioni tramite cui il destinatario può accedere all'interfaccia di GoNotice. Tra i principali canali di invio offerti vi sono email, SMS e WhatsApp. Ogni canale presenta caratteristiche uniche che consentono agli utenti di scegliere quello più adatto al tipo di comunicazione e al destinatario.

InfoCert, attualmente, si affida ai seguenti provider per l'invio della comunicazione, attraverso l'utilizzo delle licenze software open source o delle API messe a disposizione del provider come descritto di seguito:

- **SMS** – Twilio – Licenza MIT Open Source
- **Email –** Amazon SES (simple email service) - Amazon BOTO – Licenza Open source Apache License 2.0
- **Whatsapp** - REST API

I manuali operativi e le policy d'uso, che includono le obbligazioni delle parti nell'utilizzo del servizio sono accessibili ai rispettivi siti Web dei provider.

Inoltre, GoNotice offre la possibilità di configurare un canale secondario per garantire la consegna dei messaggi anche in situazioni critiche o impreviste. Il canale secondario entra in azione nel caso in cui l'invio attraverso il canale principale incontrasse delle difficoltà, come ad esempio problemi tecnici o indisponibilità di un servizio esterno come, ad esempio, la mail server del destinatario. Configurando un canale secondario, gli utenti possono assicurarsi che il messaggio venga comunque recapitato al destinatario, garantendo continuità e affidabilità nella comunicazione.

4.8 Ricezione del messaggio

Quando GoNotice crea una campagna di comunicazione, genera una prova iniziale per tracciare l'inizio del processo. Successivamente, ogni interazione correlata a questa campagna genera ulteriori evidenze, fornendo una traccia completa delle attività svolte.

Queste interazioni possono includere la ricezione della comunicazione da parte del server remoto, l'apertura del messaggio da parte del destinatario o il download di eventuali allegati. È importante notare che tutte queste evidenze sono conformi agli standard stabiliti dall'ETSI (European Telecommunications Standards Institute). Pertanto, ogni feedback ricevuto dai sistemi esterni e dal destinatario stesso genererà ulteriori evidenze, contribuendo a fornire una panoramica dettagliata e accurata dell'intero processo di comunicazione.

4.9 Evidenze

Le evidenze iniziano a essere generate al momento della creazione della campagna e dell'aggiunta dei destinatari. Quando la campagna di comunicazione viene accettata e pianificata, GoNotice crea l'evidenza SubmissionAcceptance . Quando la notifica è pronta per essere inviata, GoNotice contatta il server o il provider destinatario e, una volta ricevuta la conferma dal server, viene generata l'evidenza NotificationForAcceptance (Tabella 6). Se è configurato per attestare la visualizzazione degli allegati, GoNotice genera l'evidenza ContentHandover, che conferma l'avvenuta visualizzazione degli allegati configurati nella comunicazione.

Tutti gli ulteriori eventi relativi al processo sono tracciati in linea con le disposizioni di cui alla normativa ETSI applicabile.

4.9.1 Eventi certificati

Quando viene configurato un modello per inviare una comunicazione, l'utente-sender ha la possibilità di scegliere il tipo di certificazione che desidera ottenere per quel processo di comunicazione.

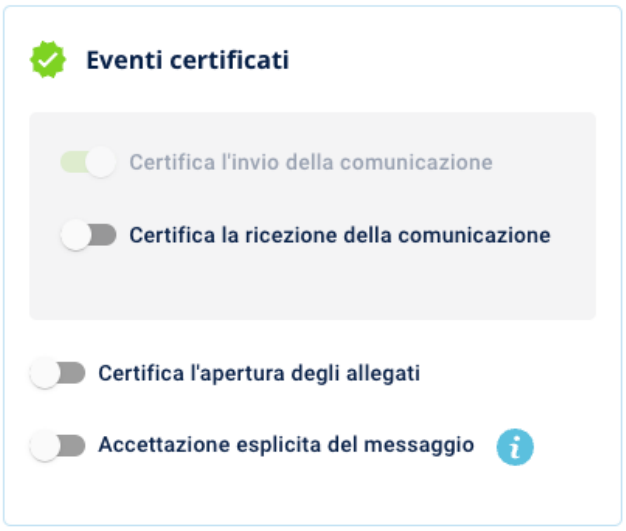

Figura 3 - Configurazione degli eventi certificati

4.9.1.1 Certifica la ricezione della comunicazione

La certificazione offerta da GoNotice attesta ufficialmente la ricezione della comunicazione da parte del destinatario. Quando abilitato, vengono prodotte le evidenze ContentAccessTracking o NotificationAccessTracking a seconda della tipologia di messaggio.

4.9.1.2 Certifica l'apertura degli allegati

La funzione di certificazione dell'apertura degli allegati attesta che il destinatario ha effettivamente aperto i file allegati alla comunicazione. Questo offre una prova concreta e verificabile che il contenuto allegato è stato visualizzato, aggiungendo un ulteriore livello di trasparenza e controllo. Tale certificazione è particolarmente utile per garantire la tracciabilità e la conformità in contesti dove è cruciale sapere che il destinatario non solo ha ricevuto, ma anche aperto e visualizzato gli allegati della comunicazione. Quando abilitato, viene prodotta la evidenza ContentHandover (.

4.9.1.3 Accettazione esplicita del messaggio

La funzione di accettazione esplicita del messaggio consente di ottenere una conferma chiara e verificabile che il destinatario ha accettato consapevolmente la comunicazione. Questo meccanismo richiede al destinatario di compiere un'azione specifica per confermare la ricezione e l'accettazione del messaggio, garantendo così che il messaggio non solo è stato ricevuto, ma anche accettato con piena consapevolezza. Quando abilitato, viene prodotta l'evidenza ConsignmentAcceptance o ConsignmentRejection, a seconda di come il destinatario interagisce con il sistema.

4.9.2 Evidenze supportate da GoNotice

La seguente classificazione degli eventi è implementata da GoNotice in piena conformità con i pertinenti standard ETSI.

Evidenza ETSI	Descrizione
SubmissionAcceptance	**Il messaggio originale è stato inviato con successo all'S-ERDS dal mittente.**
SubmissionRejection	**Il contenuto dell'utente-sender che è stato inviato all'S-ERDS dal**

Evidenza ETSI	Descrizione
	mittente non è stato accettato dall'S-ERDS.
NotificationForAcceptance	**L'R-ERDS ha notificato al destinatario la disponibilità di un messaggio (senza necessariamente rivelare il mittente, il contenuto, ecc.) e ha chiesto la disponibilità del destinatario ad accettarlo.**
RelayToNonERDS	**Un contenuto dell'utente-sender è stato inoltrato con successo a un sistema non ERDS per la consegna.**
NotificationForAcceptanceFailure	**Il destinatario non ha potuto essere notificato (o è chiaro che sarà impossibile notificare il destinatario) entro un determinato periodo di tempo a causa di errori tecnici e/o altre ragioni, oppure non esiste alcuna prova di notifica entro il periodo di tempo dato. Questo periodo di tempo può essere determinato dalla legislazione, dalle regole di politica dell'R-ERDS o dai parametri forniti dal mittente o dall'S-ERDS.**
RelayToNonERDSFailure	**Il tentativo di inoltrare un contenuto dell'utente-sender a un sistema non ERDS è fallito a causa di errori tecnici e/o altre ragioni.**
ConsignmentAcceptance	**Il destinatario ha eseguito un'azione esplicita indicando all'ERDS che ha emesso la notifica l'accettazione di ricevere un contenuto dell'utente.**
ConsignmentRejection	**Il destinatario, dopo una corretta identificazione e autenticazione, ha eseguito un'azione esplicita indicando all'R-ERDS il rifiuto di ricevere un contenuto dell'utente.**
ContentHandover	**Le prove correlate attestano che il contenuto dell'utente, in un momento specifico indicato dalle prove, ha attraversato il confine dell'R-ERDS ed è stato consegnato all'UA/Applicazione del destinatario dopo un'adeguata autenticazione.**
ConsignmentNotificationFailure	**Indica che la consegna del messaggio è fallita. Ciò può accadere a causa di un timeout nella consegna del messaggio quando scade il limite di tempo della campagna e il destinatario non ha ancora completato la politica di invio.**

Tabella 4- Evidenze ETSI supportate da GoNotice

Al fine di implementare funzionalità aggiuntive non esplicitamente previste dagli standard ETSI, viene aggiunta la seguente evidenza:

Evidenza ETSI	Descrizione
ContentAccessTracking	Il destinatario ha aperto e letto l'email, che contiene la comunicazione nel suo contenuto. Questa comunicazione non include un link a GoNotice (lato destinatario). **Questa evidenza è utilizzata solo quando l'OTP (one-time password) è disabilitato.**
NotificationAccessTracking	Il destinatario apre un'email che contiene un link che punta al sistema del destinatario. Questa evidenza è applicabile solo quando la comunicazione include un livello di certificazione di accettazione esplicita, quando vi è evidenza che l'allegato è stato aperto e/o quando l'OTP è abilitato.
FailoverSubmission	Il canale principale di comunicazione non era accessibile a causa di un errore tecnico (ad esempio, l'indirizzo email non esiste o il server è inattivo). Viene attivato il canale di fallback per la comunicazione. Questa evidenza è applicabile solo quando è stato configurato un canale secondario per la consegna.

Tabella 5 - Evidenze create in piena conformità ETSI

4.9.3 Visualizzazione

Una volta completato il processo di invio, sia che ciò avvenga per il completamento della politica di invio, per un timeout o per errori, verrà abilitato un tasto "audit".

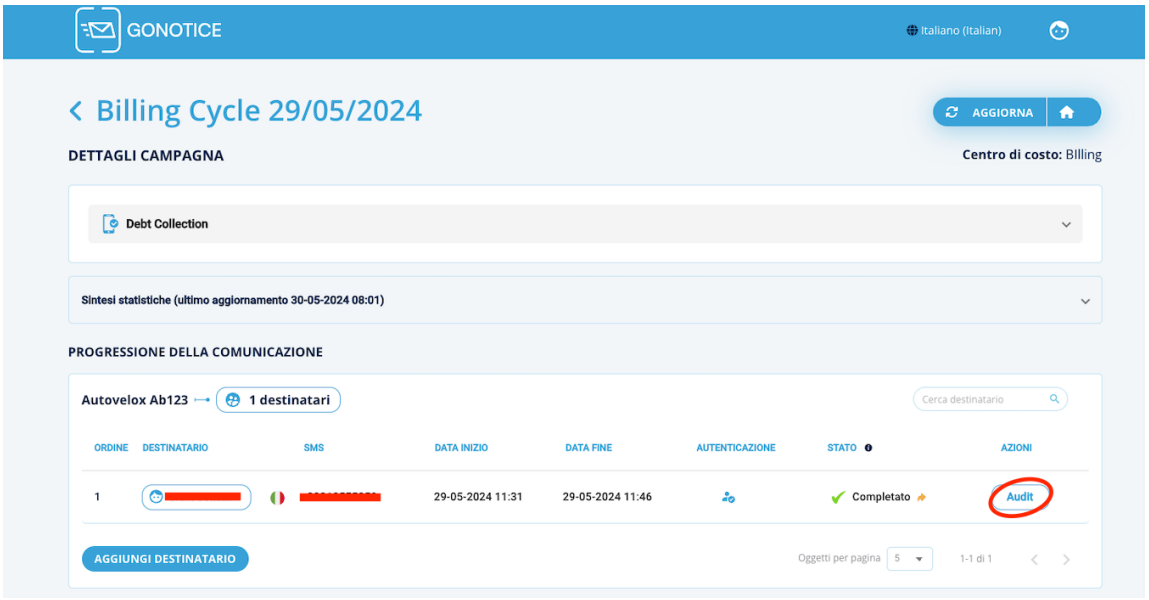

Figura 4 - Cruscotto gestione comunicazioni e tasto Audit

Quando questo tasto viene premuto, verrà scaricato un report, firmato digitalmente, in formato PDF. All'interno di questo report, si trova un sommario dettagliato di tutto ciò che è accaduto durante il processo di comunicazione, fornendo una panoramica chiara e comprensibile delle attività e degli esiti delle operazioni di invio.

Oltre al sommario, il report PDF include anche tutte le evidenze generate durante il processo, allegate in formato XML. Queste evidenze contengono informazioni precise e dettagliate che documentano ogni fase del processo di invio. Utilizzando un software apposito, è possibile estrarre e visualizzare queste evidenze per un'analisi più approfondita. Questo sistema di reportistica garantisce trasparenza e tracciabilità, consentendo di verificare e comprendere ogni aspetto della comunicazione inviata tramite GoNotice.

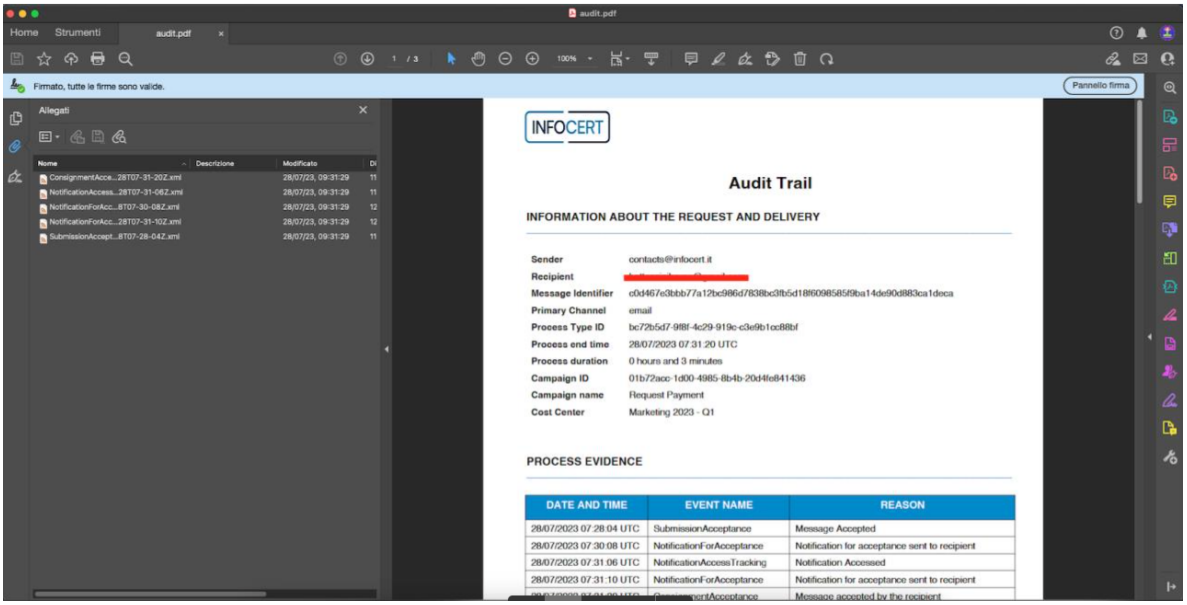

Figura 5 – Audit Trail

4.9.4 Conservazione Evidenze

Tutte le evidenze generate da GoNotice sono archiviate e sottoposte a una politica di retention che garantisce la loro conservazione per un periodo di 20 (venti) anni.

Tutte le evidenze relative ai riconoscimenti del mittente e destinatario sono archiviate e sottoposte a una politica di retention che garantisce la loro conservazione per un periodo di 20 (venti) anni.

Questo significa che ogni interazione, evento o attività relativa alle comunicazioni inviate tramite la piattaforma viene accuratamente registrata e mantenuta accessibile per un arco di tempo sufficiente a soddisfare eventuali esigenze di verifica, audit o conformità normativa.

5 MONITORAGGIO DELL'UTILIZZO DEL SISTEMA

5.1 LOG di accesso

I log di accesso sono gestiti tramite il software Keycloak, un'applicazione open source per la gestione dell'identità e degli accessi. Inizialmente, i log rimangono salvati su Keycloak, dopodiché vengono trasferiti su un database di retention, dove vengono conservati per almeno 2 (due) anni.

Tuttavia, nel caso di autenticazione tramite SPID/CIE, la gestione dei log di accesso non è gestita da Keycloak, bensì da eID Gateway, un progetto creato per centralizzare la gestione dell'accesso. Una volta effettuato l'accesso, sarà eID Gateway ad occuparsi della retention dei log di accesso per almeno 2 (due) anni.

5.2 LOG di invio

Durante l'utilizzo di GoNotice, ogni attività e ogni evento rilevante sono registrati e archiviati come log.

Questi log servono per tracciare l'utilizzo del sistema, monitorare le performance e identificare eventuali problemi. Per garantire un'archiviazione affidabile e duratura di tali dati, GoNotice utilizza Amazon CloudWatch come piattaforma di registrazione. CloudWatch offre una soluzione robusta e scalabile per la gestione dei log, consentendo di conservare i dati per lunghi periodi di tempo. In particolare, i log generati da GoNotice vengono mantenuti su CloudWatch per almeno 2 (due) anni, garantendo un accesso a lungo termine a tutte le informazioni rilevanti sull'utilizzo della piattaforma.

5.3 Servizio di monitoring

Per verificare la disponibilità del servizio sono state attivate sonde Web e strumenti di Event Management che, a fronte di componenti non disponibili, provvedono ad allertare sistemisti ed operatori.

Ognuno di questi strumenti, qualora rilevi un malfunzionamento, provvede ad allertare le figure preposte al fine che vengano attuate le contromisure previste per la tipologia di problematica riscontrata nel servizio.

In particolare, le segnalazioni delle sonde vengono analizzate dal processo di Problem Management aziendale (procedura inclusa nelle procedure aziendali certificate Vision 2000); il processo prevede la produzione di specifici output.

6 LIVELLI DEL SERVIZIO

6.1 Livelli di servizio

Qualora non diversamente specificato dalle Condizioni Generali di Contratto i livelli di servizio previsti sono dalle 0.00 alle 24.00, 7 giorni su 7 (disponibilità minima 99%).

6.2 Servizi di terze parti

Per l'erogazione del servizio di recapito certificato qualificato InfoCert si avvale di servizi di terze parti che garantiscono alta affidabilità e resilienza:

- Cloud pubblico AWS per l'erogazione del servizio. L'architettura prevede l'utilizzo di servizi gestiti per container, storage, backup, .etc., con attivazione dei micro servizi in più avalability zones delle Region AWS scelte (Region attualmente utilizzate Dublin).
- Twilio per invio notifiche via SMS
- AWS SES per invio notifiche via mail
- Whatsapp API per invio delle notifiche
- KeyCloak, come servizio per l'autenticazione di utenti (IdP oAuth 2.0) e Token

- Kong per l'esposizione delle API di servizio

Vengono inoltre utilizzati servizi di backup immutabile degli storage usati per dati applicativi, contenuti ed evidenze.

6.3 Servizi di emergenza

Al fine di garantire il corretto completamento gestione dei contenuti ed il rilascio delle relative evidenze (QERDS Evidences) sono state predisposte le seguenti soluzioni tecniche ed organizzative.

- **Utilizzo di sistemi ad alta disponibilità su Cloud AWS**, con una architettura a microservizi attivi su più availability zones, in modo da garantire l'alta affidabilità del servizio.
- **Strumenti di controllo automatico**: sono attivi nel sistema di recapito certificato qualificato strumenti automatici di verifica del sistema e delle varie componenti funzionali. In base ai problemi rilevati il sistema prevede azioni per la risoluzione degli stessi o la notifica ad operatori per consentirne l'intervento
- **Gestione dei disastri**: il QERDS InfoCert ha adottato le procedure necessarie a garantire la continuità del servizio anche in situazioni di elevata criticità – si veda per i dettagli il documento di continuità operativa del servizio GoNotice.

7 MISURE DI SICUREZZA E CONTROLLI

7.1 Generalità

Il QERDS InfoCert ha realizzato un sistema di sicurezza del sistema informativo relativo al servizio di recapito certificato qualificato.

Il sistema di sicurezza implementato è articolato su più livelli tra cui:

- L'utilizzo di un Cloud pubblico (AWS), che garantisce la resilienza e la sicurezza dei servizi in esso caricati.
- un livello procedurale e logistico, con aspetti prettamente organizzativi
- un livello logico, tramite la predisposizione di misure tecnologiche hardware e software che affrontano i problemi e i rischi connessi con la tipologia del servizio.

Tale sistema di sicurezza è realizzato per evitare rischi derivanti dal malfunzionamento dei sistemi, della rete e delle applicazioni, oltre che dall'intercettazione non autorizzata o dalla modifica dei dati.

Tutti i processi operativi del QERDS InfoCert nella erogazione del servizio di recapito certificato qualificato sono conformi al Piano di qualità aziendale.

Un estratto della politica di sicurezza InfoCert è disponibile facendone richiesta alla casella di recapito certificato qualificato InfoCert@legalmail.it.

Le politiche di sicurezza in InfoCert sono sottoposte a review non meno che annualmente, vengono inoltre aggiornate a fronte di ogni cambiamento significativo. Ogni review viene tracciata all'interno del documento stesso quand'anche non sia stato necessario apportare alcuna modifica.

7.2 Sicurezza fisica

La sicurezza fisica è demandata al servizio Cloud AWS.

Attualmente la region di erogazione è Dublino, con i servizi attivi distribuiti su tre availability zone.

AWS dispone di certificazioni di conformità ai sensi degli standard ISO/IEC 27001:2022, 27017:2015, 27018:2019 e ISO/IEC 9001:2015 e le sue pratiche sono pubblicamente disponibili sul sito Web: Il manuale operativo di AWS EC2 è pubblicamente disponibile sul sito Web: https://docs.aws.amazon.com/ Il manuale operativo di AWS EC2 è pubblicamente disponibile sul sito Web: https://docs.aws.amazon.com/ Il manuale operativo di AWS EC2 è pubblicamente disponibile sul sito Web: https://docs.aws.amazon.com/

7.2.1 Backup dei dati

In analogia con quanto previsto per le Certification Authority, anche per i sistemi di recapito certificato qualificato sono eseguiti regolarmente i backup dei file system, utilizzati dalle diverse piattaforme presenti all'interno del CED.

InfoCert fa uso delle più moderne infrastrutture per l'esecuzione di salvataggi dei contenuti dei dischi. I prodotti utilizzati per la gestione dei backup controllano e gestiscono l'esecuzione dei salvataggi e la loro archiviazione.

Le politiche di backup prevedono salvataggio delle caselle di posta con frequenza settimanale; è inoltre previsto un salvataggio incrementale giornaliero.

Il tempo di ritenzione di un salvataggio è mensile.

7.3 Controlli procedurali e sicurezza logica

7.3.1 Ruoli chiave

I ruoli chiave sono coperti da figure dotate dei necessari requisiti di esperienza, professionalità e competenza tecnica e giuridica, che vengono continuamente verificati mediante le valutazioni annuali.

La lista dei nomi e l'organigramma delle figure in ruolo chiave è stata depositata presso AgID in occasione del primo accreditamento e viene costantemente tenuta aggiornata per seguire la naturale evoluzione dell'organizzazione aziendale.

7.3.2 Accesso ai sistemi

L'accesso ai sistemi è consentito solo al personale autorizzato.

Gli operatori hanno diritto di accesso ai sistemi con le autorizzazioni minime necessarie allo svolgimento delle proprie mansioni.

I sistemi mantengono traccia degli accessi e delle operazioni effettuate.

7.3.3 Regole comportamentali

Le Politiche di Sicurezza di InfoCert e i documenti collegati illustrano le linee guida e la policy aziendale per tutti i servizi presenti in azienda. Tali documenti hanno l'obiettivo di creare una maggiore coscienza e considerazione in tutto il personale, circa la riservatezza delle informazioni e delle attività effettuate durante l'orario d'ufficio. Il personale viene esplicitamente invitato "alla massima riservatezza" riguardo a tutte le informazioni di cui venga in possesso. Sono indicate le norme per l'accesso fisico dei dipendenti e dei consulenti esterni, le norme per l'utilizzo del badge, e le regole per l'accesso fuori orario. Parte dei documenti sono dedicati alla sicurezza delle apparecchiature, dei sistemi e delle applicazioni informatiche. Sono indicate le norme circa l'uso della password (segretezza e necessità di cambiarla periodicamente) e del PC (utilizzo limitato all'uso professionale, cura e responsabilità della macchina, divieto di utilizzo di software non rilasciato dall'apposito ufficio, norme per la connessione remota, norme per la gestione dei virus, norme per l'accesso ad Internet e per l'utilizzo della posta elettronica, rimozione immediata degli accessi qualora non più necessari). Obiettivo delle politiche in essi espresse è, anche, minimizzare la possibilità che software illegale o non autorizzato possa essere introdotto, anche involontariamente, nella rete interna.

Tutti i documenti non riservati rivolti al personale sono disponibili nella Intranet aziendale.

7.3.4 Raccomandazioni per il Titolare

Il *Titolare* deve custodire in maniera sicura le credenziali e gli strumenti di autenticazione al servizio; deve utilizzare il servizio per le sole modalità previste dal Manuale Operativo e dalle vigenti leggi nazionali e internazionali.

È opportuno dotare le stazioni di lavoro di un antivirus costantemente aggiornato per garantire maggiore sicurezza per quanto viene spedito e ricevuto.

7.4 Controllo del personale

7.4.1 Qualifiche, esperienze e autorizzazioni richieste

Effettuata la pianificazione annuale delle Risorse Umane, il Responsabile Funzione/Struttura Organizzativa identifica le caratteristiche e le skill della risorsa da inserire (job profile). Successivamente, di concerto con il responsabile selezione, viene attivato il processo di ricerca e selezione.

7.4.2 Procedure di controllo delle esperienze pregresse

I candidati individuati partecipano al processo di selezione affrontando un primo colloquio conoscitivo-motivazionale con il responsabile della selezione e un successivo colloquio tecnico con il responsabile di Funzione/Struttura Organizzativa, volto a verificare le skill dichiarate dal candidato. Ulteriori strumenti di verifica sono esercitazioni e test.

7.4.3 Requisiti di formazione

A garanzia che nessun individuo possa singolarmente compromettere o alterare la sicurezza globale del sistema oppure svolgere attività non autorizzate, è previsto di affidare la gestione operativa del sistema a persone diverse, con compiti separati e ben definiti. Il personale addetto alla progettazione ed erogazione del servizio di recapito certificato qualificato è un dipendente InfoCert ed è stato selezionato in base alla esperienza nella progettazione, realizzazione e conduzione di servizi informatici, con caratteristiche di affidabilità e riservatezza. Interventi di formazione sono pianificati periodicamente per sviluppare la consapevolezza dei compiti assegnati. In particolare, prima dell'inserimento del personale nell'attività operativa, sono realizzati interventi formativi allo scopo di fornire ogni competenza (tecnica, organizzativa e procedurale) necessaria a svolgere i compiti assegnati.

7.4.4 Frequenza di aggiornamento della formazione

Ogni inizio anno viene svolta l'analisi delle esigenze formative propedeutica alla definizione delle attività formative da erogare nell'anno. L'analisi è strutturata nel modo seguente:

Incontro con la Direzione per la raccolta dei dati relativi alle esigenze formative necessarie per raggiungere gli obiettivi aziendali;
Intervista ai Responsabili per la rilevazione delle esigenze formative specifiche delle proprie aree;
Restituzione dei dati raccolti alla Direzione Aziendale per chiusura ed approvazione del Piano Formativo.

Entro il mese di febbraio il Piano Formativo così definito viene condiviso e reso pubblico.

7.4.5 Frequenza nella rotazione dei turni di lavoro

La presenza in sede o in modalità di lavoro agile (smart working) si distribuisce su una fascia oraria dalle ore 08:00 alle ore 19:00 dal lunedì al venerdì.

Il presidio degli ambienti di produzione nella fascia notturna e nella fascia festiva viene garantito attraverso un piano di turnazione della reperibilità predisposto dal responsabile di unità organizzativa mensilmente con un anticipo di almeno 10 giorni. A seconda della necessità, gli interventi potranno essere condotti da remoto (teleintervento) o richiedere l'accesso alle sedi.

Fermo restando il possesso dei necessari requisiti tecnici e professionali, l'Azienda provvede ad avvicendare nella reperibilità il maggior numero possibile di lavoratori, dando priorità ai dipendenti che ne facciano richiesta.

7.4.6 Sanzioni per azioni non autorizzate

Si fa riferimento al "CCNL Metalmeccanici e installazione impianti industria privata" per la procedura di irrogazione delle sanzioni.

7.4.7 Controlli sul personale non dipendente

L'accesso al personale non dipendente è regolato da una specifica policy aziendale.

7.4.8 Documentazione che il personale deve fornire

Al momento dell'assunzione, il dipendente deve fornire copia di un documento d'identità valido, copia della tessera sanitaria valida e una foto in formato tessera per il badge di accesso ai locali. Dovrà in seguito compilare e firmare il consenso al trattamento dei dati personali e l'impegno a non divulgare notizie e/o documenti riservati. Dovrà infine prendere visione del Codice Etico e della Netiquette InfoCert.

7.5 Compromissione del servizio e business continuity

7.5.1 Procedure per la gestione degli incidenti

Il QERDS InfoCert ha descritto le procedure di gestione degli incidenti nell'ambito del SGSI certificato ISO 27000. Ogni eventuale incidente, non appena rilevato, è soggetto a puntuale analisi, individuazione delle contromisure correttive e verbalizzazione da parte del responsabile del servizio. Il verbale è firmato digitalmente; una copia è inviata anche a AgID, unitamente alla dichiarazione delle azioni di intervento mirate a eliminare le cause che possono aver dato luogo all'incidente, se sotto il controllo di InfoCert conforme all'articolo 19 del Regolamento.

7.5.2 Corruzione delle chiavi, del software o dei dati

Per aumentare la resilienza in caso di problemi o compromissione della chiave utilizzata per la firma delle evidenze, InfoCert ha predisposto due chiavi e certificati differenti, con tecnologie di cifratura differenti (RSA 2048 e Curve Ellittiche). In casi di compromissione di una delle chiavi si prevede di sospenderne l'uso e di utilizzare solo la chiave non compromessa.

Tutte le evidenze del sistema di recapito certificato qualificato vengono portate nel sistema di conservazione InfoCert, garantendo integrità e disponibilità anche in caso di compromissione della chiave utilizzata o del servizio.

I dati vengono gestiti, all'interno del servizio QERDS, in modalità sicura su storage ridondati, gestiti dal Cloud Provider, con attivi backup immutabili per garantire il massimo della sicurezza.

Il software è gestito secondo procedure standard secondo i sistemi di qualità ISO 9000.

7.5.3 Servizi di firma e marcatura

Il servizio QERDS utilizza nella gestione dei contenuti e delle evidenze, la firma elettronica qualificata e il servizio di marcatura temporale InfoCert, garantendo quindi il massimo in termini di sicurezza e resilienza del servizio.

7.6 Cessazione del servizio di prestatore o provider di servizio

InfoCert ha previsto un piano di terminazione per tutti i casi, schedulati e non schedulati, in cui sia necessario interrompere l'erogazione del servizio QERDS.

Nel caso di cessazione dell'attività di QERDS Provider, InfoCert comunicherà questa intenzione all'Autorità di vigilanza (AgID) e l'ente di certificazione (CAB) con un anticipo di almeno 6 (sei) mesi, indicando, eventualmente, il QERDS Provider sostitutivo. Con pari anticipo InfoCert

informa della cessazione delle attività tutti i Titolari del servizio di recapito certificato qualificato attivi.

Nella comunicazione, nel caso in cui non sia indicato un provider sostitutivo, sarà chiaramente specificato le modalità operative per l'accesso alle informazioni (evidenze) ancora in carico al gestore.

Si veda il documento QERDS Termination Plan dei Servizi di recapito certificato qualificato GoNotice disponibile presso il certificatore qualificato.

7.7 Controlli sulla sicurezza informatica

7.7.1 Requisiti di sicurezza specifici dei server

Il sistema operativo dei dispositivi, dei server e degli elaboratori utilizzati nelle attività di setup, gestione ed erogazione del servizio di recapito certificato qualificato sono messi in sicurezza (hardening), sono cioè configurati, in modo da minimizzare l'impatto di eventuali vulnerabilità eliminando tutte le funzionalità che non servono per il funzionamento e la gestione del servizio stesso.

7.7.2 Valutazioni di vulnerabilità

InfoCert svolge periodicamente delle valutazioni sulle vulnerabilità del Sistema (vulnerability assessment) e test antiintrusione (penetration test). A fronte dei risultati mette in atto tutte le contromisure per mettere in sicurezza le applicazioni.

7.7.3 Requisiti di sicurezza relativi agli amministratori dei sistemi

L'accesso da parte degli Amministratori di sistema, all'uopo nominati in conformità con quanto prescritto dalla normativa vigente, avviene tramite applicazioni dedicate e predisposte per mantenere l'appropriato livello di sicurezza e i privilegi ad agire sui sistemi, sulle configurazioni e sulle applicazioni solo previa autenticazione individuale. Gli accessi sono tracciati e loggati e conservati per 12 mesi.

8 CONTROLLI E VALUTAZIONI DI CONFORMITÀ

Per ottenere la qualifica di prestatore di servizi fiduciari qualificati e non, in conformità al Regolamento eIDAS 0 è necessario espletare l'iter previsto dall'articolo 21 del suddetto Regolamento.

InfoCert ha presentato ad AgID l'apposita richiesta per ottenere il riconoscimento di "prestatore del servizio fiduciario qualificato" allegando un report della valutazione di conformità con il Regolamento (Conformity Assesment Report - CAR) rilasciato da un organismo di valutazione autorizzato dal preposto organismo nazionale (CAB), che in Italia è ACCREDIA.

InfoCert presta il Servizio quale prestatore di servizi fiduciari qualificati ai sensi del Regolamento (UE) N. 910/2014 [1] del 23/07/2014, sulla base di una valutazione di conformità effettuata dal Conformity Assessment Body CSQA Certificazioni S.r.l., ai sensi del Regolamento di cui sopra e

della Norma ETSI EN 319 401[5] secondo lo schema di valutazione eIDAS 0[1] definito da ACCREDIA a fronte delle norme ETSI EN 319_403[9] e UNI CEI EN ISO/IEC 17065:2012.

8.1 Frequenza o circostanze per la valutazione di conformità

La valutazione di conformità viene ripetuta ogni 2 (due) anni, ma ogni anno il CAB esegue un audit di sorveglianza.

8.2 Identità e qualifiche di chi effettua il controllo

Il controllo viene effettuato da:

Denominazione sociale	**CSQA Certificazioni S.r.l.**
Sede legale	**Via S. Gaetano n. 74, 36016 Thiene (VI)**
N. di telefono	**+39 0445 313011**
N. Iscrizione Registro Imprese	**Business Register no. 02603680246/REA no. 258305**
Partita IVA/Codice Fiscale	**02603680246**
Website	**https://www.csqa.it**

8.3 Rapporti tra InfoCert e CAB

InfoCert e CSQA non hanno interessi finanziari né relazioni di affari.

Non sono in corso rapporti commerciali o di partnership che possono creare pregiudizi a favore o contro InfoCert nella valutazione obiettiva di CSQA.

8.4 Aspetti oggetto di valutazione

Il CAB è chiamato a valutare la conformità rispetto al Manuale Operativo, al Regolamento e alla normativa applicabile delle procedure adottate, dell'organizzazione del QERDS InfoCert, dell'organizzazione dei ruoli, della formazione del personale, della documentazione contrattuale.

8.5 Azioni in caso di non conformità

In caso di non conformità, il CAB deciderà se inviare comunque il rapporto ad AgID, o se riservarsi di rieseguire l'audit dopo che la non conformità sia stata sanata.

InfoCert si impegna a risolvere tutte le non conformità in maniera tempestiva, mettendo in atto tutte le azioni di miglioramento e adeguamento necessarie.

9 ALTRI ASPETTI LEGALI E DI BUSINESS

9.1 Copertura assicurativa

Il TSP InfoCert ha stipulato un contratto assicurativo per la copertura dei rischi dell'attività e dei danni causati a terzi, che ha come massimali:

- 10.000.000 euro per singolo sinistro;
- 10.000.000 euro per annualità.

9.2 Proprietà intellettuale

9.3 Rappresentanza e garanzie

InfoCert mantiene la responsabilità per l'osservanza delle procedure prescritte nella propria policy sulla sicurezza delle informazioni, anche quando alcune funzioni vengono delegate ad un altro soggetto, ai sensi dell'art. 2.4.1. dell'Allegato al Regolamento di esecuzione UE 2015/1502 della Commissione.

Il Titolare è responsabile della veridicità dei dati comunicati nella Richiesta di Attivazione al servizio. Qualora lo stesso, al momento dell'identificazione, abbia, anche attraverso l'utilizzo di documenti personali non veri, celato la propria reale identità o dichiarato falsamente di essere altro soggetto o, comunque, agito in modo tale da compromettere il processo di identificazione e le relative risultanze indicate nel certificato, sarà considerato responsabile di tutti i danni derivanti al QERDS InfoCert e/o a terzi dall'inesattezza delle informazioni contenute nella richiesta, con obbligo di garantire e manlevare il QERDS InfoCert da eventuali richieste di risarcimento danni.

Il Titolare è responsabile dei danni derivanti al QERDS InfoCert e/o a terzi nel caso di ritardo da parte loro dell'attivazione delle procedure previste nel paragrafo §3.5.2 del presente Manuale Operativo (revoca e sospensione del servizio).

9.4 Canali di comunicazione ufficiali

Si rimanda alle procedure e ai canali di contatto presenti nel paragrafo §1.4 ed in particolare al Responsabile del Manuale Operativo indicato nel paragrafo §1.4.2.

APPENDICE A - CERTIFICATI FIRMA UTILIZZATI DA QERDS

Electronic Signature Signing Certificate - RSA

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 28666201 (0x1b56959)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer:  C=IT,  O=InfoCert  S.p.A.,  OU=Qualified  Trust  Service  Provider/2.5.4.97=VATIT-
07945211006, CN=InfoCert Qualified Electronic Signature CA 3
        Validity
            Not Before: Jun  5 15:05:04 2024 GMT
            Not After : Jun  5 00:00:00 2027 GMT
        Subject:  CN=InfoCert  QERDS  GoNotice/2.5.4.97=NTRIT-07945211006,  C=IT,  L=ROMA,  O=InfoCert
S.p.A./dnQualifier=8d3e3081-f168-492f-983f-ec4155009b87
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:ab:c3:4b:1d:27:c9:4e:cb:39:27:cd:8e:78:4f:
                    d2:21:b6:ee:5c:9e:64:56:e6:66:4c:3e:2f:c1:fb:
                    54:d7:29:e5:26:e3:e4:6e:3b:2c:e1:70:d0:25:6b:
                    1a:c9:f5:94:93:a9:fb:ff:2d:07:32:11:8e:e9:fc:
                    81:2b:89:de:8d:b3:72:56:de:3d:07:c6:84:1e:ce:
                    75:f9:0c:47:d5:65:0b:20:2e:59:6f:4a:d7:b9:d2:
                    a9:1e:4e:e8:af:09:39:cc:4b:e6:c3:e7:d0:40:aa:
                    fa:3e:ab:37:95:e1:6c:54:37:5b:d5:ab:2e:01:d7:
                    36:08:cc:c1:3d:22:49:47:cc:61:99:15:c1:b5:2a:
                    c6:0c:68:f1:02:09:ec:52:9e:9d:5a:a6:d2:c4:18:
                    e0:fd:dc:90:16:a4:5e:4d:b8:38:ee:1a:2e:75:8f:
                    c3:f9:38:be:09:87:ca:64:85:10:15:5b:91:be:b7:
                    cc:9d:24:0b:6c:3b:21:e0:a4:32:3e:24:67:02:06:
                    8f:31:cc:9f:3c:03:06:55:a9:c9:5e:b3:65:37:a2:
                    d8:8a:e3:6f:40:2d:d1:61:ce:92:76:80:cf:3e:5d:
                    13:12:37:80:28:ac:37:6c:e0:5b:e9:67:67:50:69:
                    30:16:90:53:a6:4f:62:a3:0e:7a:34:1d:3d:75:50:
                    cf:df
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Authority Information Access:
                OCSP - URI:http://ocsp.qc.ca3.InfoCert.it/
                CA Issuers - URI:http://cert.InfoCert.it/ca3/qc/CA.crt

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://crl.InfoCert.it/ca3/qc/CRL39.crl

URI:ldap://ldap.InfoCert.it/cn%3DInfoCert%20Qualified%20Electronic%20Signature%20CA%203%20CRL39,ou%3
DQualified%20Trust%20Service%20Provider,o%3DINFOCERT%20SPA,c%3DIT?certificateRevocationList

            X509v3 Certificate Policies:
                Policy: 0.4.0.194112.1.3
                Policy: 1.3.76.36.1.1.46
                  CPS: http://www.firma.InfoCert.it/documentazione/manuali.php

            qcStatements:

0v0......F..0......F..0......F.....0......F..0......F...0>.....F..0402.,https://www.firma.InfoCert.i
t/pdf/PKI-DS.pdf..en
            X509v3 Key Usage: critical
                Non Repudiation
            X509v3 Authority Key Identifier:
                keyid:9B:3B:1B:18:6A:3E:A2:04:03:F4:D7:99:10:CF:97:11:4C:F1:AA:DE

            X509v3 Subject Key Identifier:
                6E:B3:BF:27:A7:32:26:BC:70:3A:F9:C9:E4:1E:13:4B:05:93:93:80
    Signature Algorithm: sha256WithRSAEncryption
         25:43:00:68:d4:db:06:d4:1d:84:50:83:28:0f:7c:1e:53:c9:
         d8:d0:5e:dd:cb:f0:54:04:5c:03:86:c5:cf:f1:c2:9b:8f:bb:
         02:71:78:63:8a:02:18:85:50:d8:1b:af:82:9e:3f:3d:7d:1c:
```

```
        fb:b7:d2:e9:70:18:c4:5f:b5:3b:36:76:17:b3:18:f7:c3:5b:
        c6:50:87:af:92:db:4d:e2:b6:94:4d:99:25:c3:8d:19:f7:12:
        cb:e6:7d:e9:ce:6a:24:68:0d:b2:02:ff:f8:94:32:39:38:84:
        80:d4:c7:8f:be:44:49:03:de:f1:68:e5:7d:0b:15:2f:7f:42:
        ed:6b:d2:37:33:20:ca:6e:8b:75:86:8a:a0:19:f8:7d:09:d7:
        ac:05:1e:18:65:6d:bb:61:13:71:b1:8c:33:4f:ba:b2:96:c3:
        8b:81:07:10:44:a6:1f:70:02:ef:02:1c:8b:43:0f:c7:9e:68:
        13:4b:c8:5d:13:5f:51:3f:51:5d:c4:4d:4b:ce:f7:e0:9f:da:
        f6:dc:1a:ec:04:2f:5c:a0:67:58:5d:6c:34:55:13:3b:49:b7:
        80:8f:b4:2f:83:b1:0a:78:60:1c:b9:31:8f:3d:fd:1f:73:a4:
        19:aa:9f:b8:b6:eb:26:5c:95:3a:31:38:bf:ab:32:48:f3:fa:
        d7:a4:98:9a:07:42:6d:83:d1:56:6b:37:25:6f:08:27:63:c0:
        66:9a:6e:4e:57:7c:11:7c:4c:1b:2e:60:94:b8:ca:9e:49:e1:
        f9:c9:15:63:e3:db:0f:1d:54:80:db:b3:82:7e:df:59:2f:55:
        bf:9d:48:6b:f2:ad:b2:b2:33:96:09:0e:22:46:fb:a3:1f:3e:
        85:48:06:49:e6:c6:59:ae:d3:14:58:b7:a1:a4:3b:99:5f:1d:
        cd:f9:de:71:5a:36:87:97:59:78:73:de:0d:df:03:b9:b2:97:
        4d:b5:3d:d9:bb:02:89:8d:e1:d0:af:4f:37:39:ae:35:8e:55:
        2a:c1:ef:48:67:21:07:fd:48:28:92:ad:73:48:0c:75:80:be:
        73:d2:83:c1:3d:0f:c8:1e:b0:e3:1f:37:6f:a3:8e:db:31:39:
        54:de:66:9b:b7:52:9b:c4:11:e4:2a:31:a8:7a:36:a7:89:d1:
        d1:2a:a2:f8:50:6a:36:25:c4:ad:e8:a6:eb:cd:ad:d5:b8:94:
        de:da:b1:34:12:73:9c:25:a6:ff:98:36:81:e2:91:08:5f:51:
        63:02:6a:f3:2f:34:18:20:05:8d:fd:71:0c:56:f7:da:3e:f2:
        6f:08:44:9b:6a:11:7a:24:29:50:9d:9f:a2:08:92:53:b7:9b:
        97:d5:06:d2:42:b6:9d:a2
```

```
-----BEGIN CERTIFICATE-----
MIIHhTCCBW2gAwIBAgIEAbVpWTANBgkqhkiG9w0BAQsFADCBpTELMAkGA1UEBhMCSVQxGDAWBgNVBAoMD0luZm9DZXJ0IFMucC5B
LjEpMCcGA1UECwwgUXVhbGlmaWVkIFRydXN0IFNlcnZpY2UgUHJvdmlkZXIxGjAYBgNVBGEMEVZBVElULTA3OTQ1MjExMDA2MTUw
MwYDVQQDDCxJbmZvQ2VydCBRdWFsaWZpZWQgRWxlY3Ryb25pYyBTaWduYXR1cmUgQ0EgMzAeFw0yNDA2MDUxNTA1MDRaFw0yNzA2
MDUwMDAwMDBaMIGjMSAwHgYDVQQDDBdJbmZvQ2VydCBRRVJEUyBHb05vdGljZTEaMBgGA1UEYQwRTlRSSVQtMDc5NDUyMTEwMDYx
CzAJBgNVBAYTAklUMQ0wCwYDVQQHDARST01BMRgwFgYDVQQKDA9JbmZvQ2VydCBTLnAuQS4xLTArBgNVBC4TJDhkM2UzMDgxLWYx
NjgtNDkyZi05ODNmLWVjNDE1NTAwOWI4NzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKvDSx0nyU7LOSfNjnhP0iG2
7lyeZFbmZkw+L8H7VNcp5Sbj5G47LOFw0CVrGsn1lJOp+/8tBzIRjun8gSuJ3o2zclbePQfGhB7OdfkMR9VlCyAuWW9K17nSqR5O
6K8JOcxL5sPn0ECq+j6rN5XhbFQ3W9WrLgHXNgjMwT0iSUfMYZkVwbUqxgxo8QIJ7FKenVqm0sQY4P3ckBakXk24OO4aLnWPw/k4
vgmHymSFEBVbkb63zJ0kC2w7IeCkMj4kZwIGjzHMnzwDBlWpyV6zZTei2Irjb0At0WHOknaAzz5dExI3gCisN2zgW+lnZ1BpMBaQ
U6ZPYqMOejQdPXVQz98CAwEAAaOCArswggK3MAkGA1UdEwQCMAAwbgYIKwYBBQUHAQEEYjBgMCsGCCsGAQUFBzABhh9odHRwOi8v
b2NzcC5xYy5jYTMuaW5mb2NlcnQuaXQvMDEGCCsGAQUFBzAChiVodHRwOi8vY2VydC5pbmZvY2VydC5pdC9jYTMvcWMvQ0EuY3J0
MIH7BgNVHR8EgfMwgfAwge2ggeqggeeGJ2h0dHA6Ly9jcmwuaW5mb2NlcnQuaXQvY2EzL3FjL0NSTDM5LmNybIaBu2xkYXA6Ly9s
ZGFwLmluZm9jZXJ0Lml0L2NuJTNESW5mb0NlcnQlMjBRdWFsaWZpZWQlMjBFbGVjdHJvbmljJTIwU2lnbmF0dXJlJTIwQ0ElMjAz
JTIwQ1JMMzksb3UlM0RRdWFsaWZpZWQlMjBUcnVzdCUyMFNlcnZpY2UlMjBQcm92aWRlcixvJTNESU5GT0NFUlQlMjBTUEEsYyUz
RElUP2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3QwZQYDVR0gBF4wXDAJBgcEAIvsQAEDME8GBitMJAEBLjBFMEMGCCsGAQUFBwIB
FjdodHRwOi8vd3d3LmZpcm1hLmluZm9jZXJ0Lml0L2RvY3VtZW50YXppb25lL21hbnVhbGkucGhwMIGEBggrBgEFBQcBAwR4MHYw
CAYGBACORgEBMAgGBgQAjkYBBDALBgYEAI5GAQMCARQwEwYGBACORgEGMAkGBwQAjkYBBgIwPgYGBACORgEFMDQwMhYsaHR0cHM6
Ly93d3cuZmlybWEuaW5mb2NlcnQuaXQvcGRmL1BLSS1EUy5wZGYTAmVuMA4GA1UdDwEB/wQEAwIGQDAfBgNVHSMEGDAWgBSbOxsY
aj6iBAP015kQz5cRTPGq3jAdBgNVHQ4EFgQUbrO/J6cyJrxwOvnJ5B4TSwWTk4AwDQYJKoZIhvcNAQELBQADggIBACVDAGjU2wbU
HYRQgygPfB5TydjQXt3L8FQEXAOGxc/xwpuPuwJxeGOKAhiFUNgbr4KePz19HPu30ulwGMRftTs2dhezGPfDW8ZQh6+S203itpRN
mSXDjRn3EsvmfenOaiRoDbIC//iUMjk4hIDUx4++REkD3vFo5X0LFS9/Qu1r0jczIMpui3WGiqAZ+H0J16wFHhhlbbthE3GxjDNP
urKWw4uBBxBEph9wAu8CHItDD8eeaBNLyF0TX1E/UV3ETUvO9+Cf2vbcGuwEL1ygZ1hdbDRVEztJt4CPtC+DsQp4YBy5MY89/R9z
pBmqn7i26yZclToxOL+rMkjz+tekmJoHQm2D0VZrNyVvCCdjwGaabk5XfBF8TBsuYJS4yp5J4fnJFWPj2w8dVIDbs4J+31kvVb+d
SGvyrbKyM5YJDiJG+6MfPoVIBknmxlmu0xRYt6GkO5lfHc353nFaNoeXWXhz3g3fA7myl021Pdm7AomN4dCvTzc5rjWOVSrB70hn
IQf9SCiSrXNIDHWAvnPSg8E9D8gesOMfN2+jjtsxOVTeZpu3UpvEEeQqMah6NqeJ0dEqovhQajYlxK3opuvNrdW4lN7asTQSc5wl
pv+YNoHikQhfUWMCavMvNBggBY39cQxW99o+8m8IRJtqEXokKVCdn6IIklO3m5fVBtJCtp2i
-----END CERTIFICATE-----
```

Electronic Signature Signing Certificate - EC

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            1c:72:de:8f:74:2e:09:a0:0e:58:31:d6:38:ff:d4:4e:4f:d2:6a:c6
    Signature Algorithm: ecdsa-with-SHA384
        Issuer:  C=IT,  O=InfoCert  S.p.A.,  OU=Qualified  Trust  Service  Provider/2.5.4.97=VATIT-
07945211006, CN=InfoCert Qualified Electronic Signature EC CA 4
        Validity
            Not Before: Jun  5 14:53:35 2024 GMT
            Not After : Jun  5 00:00:00 2029 GMT
```

```
        Subject: CN=InfoCert QERDS GoNotice/2.5.4.97=NTRIT-07945211006, C=IT, L=ROMA, O=InfoCert
S.p.A./dnQualifier=0393f379-5d48-4ce0-8922-307ca4aebd17
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:1a:b1:6d:4d:5f:7b:63:01:00:f8:8f:7e:91:59:
                    7b:9b:b7:71:ae:91:7c:b8:7f:ef:57:89:8f:55:89:
                    56:45:a4:20:af:63:de:64:4a:22:d6:b4:e6:f1:91:
                    1b:5e:39:34:c0:b2:23:5f:c7:e2:0c:89:a7:c1:84:
                    90:50:c2:99:e0
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Certificate Policies:
                Policy: 0.4.0.194112.1.3
                Policy: 1.3.76.36.1.1.46
                  CPS: http://www.firma.InfoCert.it/documentazione/manuali.php
            qcStatements:

0v0......F..0......F.....0......F..0>.....F..0402.,https://www.firma.InfoCert.it/pdf/PKI-
DS.pdf..en0......F..0......F...
            Authority Information Access:
                OCSP - URI:http://ocsp.qcec.ca4.InfoCert.it
                CA Issuers - URI:http://crl.ca4.InfoCert.it/qcec/CA.crt

            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://crl.ca4.InfoCert.it/qcec/CRL01.crl

            X509v3 Key Usage: critical
                Non Repudiation
            X509v3 Authority Key Identifier:
                keyid:8C:DF:7C:B8:F0:94:15:36:0B:7F:DF:81:71:F5:DB:41:5D:3B:FD:FC
            X509v3 Subject Key Identifier:
                E9:89:EE:6B:F7:A7:EA:A2:22:35:B2:D3:9A:6F:7E:87:7F:BA:21:16
    Signature Algorithm: ecdsa-with-SHA384
         30:65:02:30:09:aa:0d:ab:a7:6e:ed:b7:2d:f6:63:64:82:8a:
         e4:15:b2:48:24:e2:a1:0f:a3:e7:7a:5a:5d:fa:56:90:75:8f:
         df:de:a9:3f:96:98:dc:57:8f:7e:de:63:fa:4b:2f:94:02:31:
         00:9f:f6:a3:73:dc:38:bd:9e:7f:e8:9d:fb:32:62:c8:25:6a:
         26:04:03:b6:b3:08:75:17:ca:7d:1e:4f:ef:32:22:5a:df:3a:
         42:55:23:fd:99:be:eb:59:b6:42:22:8f:6e

-----BEGIN CERTIFICATE-----
MIIEbDCCA/KgAwIBAgIUHHLej3QuCaAOWDHWOP/UTk/SasYwCgYIKoZIzj0EAwMwgagxCzAJBgNVBAYTAklUMRgwFgYDVQQKDA9J
bmZvQ2VydCBTLnAuQS4xKTAnBgNVBAsMIFF1YWxpZmllZCBUcnVzdCBTZXJ2aWNlIFByb3ZpZGVyMRowGAYDVQRhDBFWQVRJVC0w
Nzk0NTIxMTAwNjE4MDYGA1UEAwwvSW5mb0NlcnQgUXVhbGlmaWVkIEVsZWN0cm9uaWMgU2lnbmF0dXJlIEVDIENBIDQwHhcNMjQw
NjA1MTQ1MzM1WhcNMjkwNjA1MDAwMDAwWjCBozEgMB4GA1UEAwwXSW5mb0NlcnQgUUVSRFMgR29Ob3RpY2UxGjAYBgNVBGEMEU5U
UklULTA3OTQ1MjExMDA2MQswCQYDVQQGEwJJVDENMAsGA1UEBwwEUk9NQTEYMBYGA1UECgwPSW5mb0NlcnQgUy5wLkEuMS0wKwYD
VQQuEyQwMzkzZjM3OS01ZDQ4LTRjZTAtODkyMi0zMDdjYTRhZWJkMTcwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAAQasW1NX3tj
AQD4j36RWXubt3GukXy4f+9XiY9ViVZFpCCvY95kSiLWtObxkRteOTTAsiNfx+IMiafBhJBQwpngo4IB+zCCAfcwCQYDVR0TBAIw
ADBlBgNVHSAEXjBcMAkGBwQAi+xAAQMwTwYGK0wkAQEuMEUwQwYIKwYBBQUHAgEWN2h0dHA6Ly93d3cuZmlybWEuaW5mb2NlcnQu
aXQvZG9jdW1lbnRhemlvbmUvbWFudWFsaS5waHAwgYQGCCsGAQUFBwEDBHgwdjAIBgYEAI5GAQEwCwYGBACORgEDAgEUMAgGBgQA
jkYBBDA+BgYEAI5GAQUwNDAyFixodHRwczovL3d3dy5maXJtYS5pbmZvY2VydC5pdC9wZGYvUEtJLURTLnBkZhMCZW4wEwYGBACO
RgEGMAkGBwQAjkYBBgIwcAYIKwYBBQUHAQEEZDBiMCwGCCsGAQUFBzABhiBodHRwOi8vb2NzcC5xY2VjLmNhNC5pbmZvY2VydC5p
dDAyBggrBgEFBQcwAoYmaHR0cDovL2NybC5jYTQuaW5mb2NlcnQuaXQvcWNlYy9DQS5jcnQwOgYDVR0fBDMwMTAvoC2gK4YpaHR0
cDovL2NybC5jYTQuaW5mb2NlcnQuaXQvcWNlYy9DUkwwMS5jcmwwDgYDVR0PAQH/BAQDAgZAMB8GA1UdIwQYMBaAFIzffLjwlBU2
C3/fgXH120FdO/38MB0GA1UdDgQWBBTpie5r96fqoiI1stOab36Hf7ohFjAKBggqhkjOPQQDAwNoADBlAjAJqg2rp27tty32Y2SC
iuQVskgk4qEPo+d6Wl36VpB1j9/eqT+WmNxXj37eY/pLL5QCMQCf9qNz3Di9nn/onfsyYsglaiYEA7azCHUXyn0eT+8yIlrfOkJV
I/2ZvutZtkIij24=
-----END CERTIFICATE-----
```