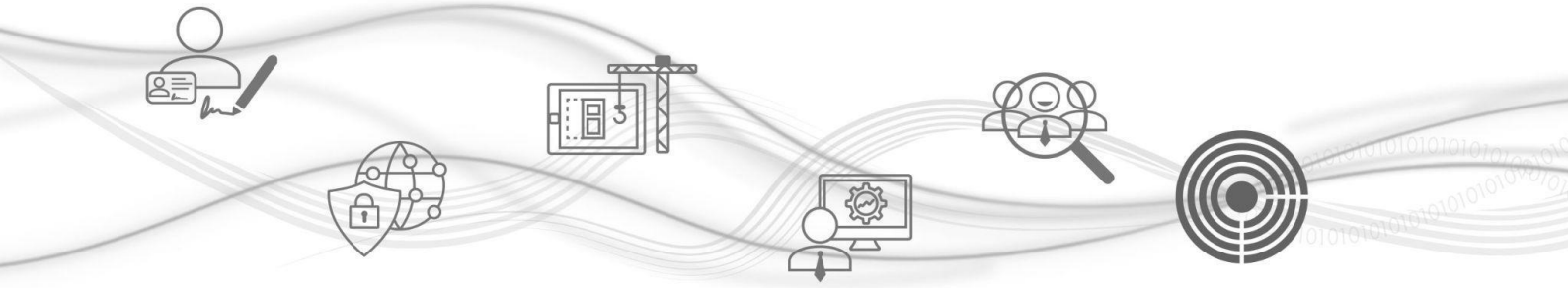
Manuale Operativo

Certificate Policy & Certificate Practice Statement per i Servizi di Certificazione e Marcatura Temporale



Categoria	**Manuale Operativo**	Codice Documento	**NAM-MO-FDMT-**	**Namirial S.p.A.**
Redatto da	**Margherita Menghini**	Nota di riservatezza	**Documento Pubblico**	**Il Legale Rappresentante**
Verificato da	**Franco Tafini**	Versione	**3.2**	**Massiliano Pellegrini**
Approvato da	**Massimiliano Pellegrini**	Data di emissione	**26/02/2023**	—

Signed by: PELLEGRINI MASSIMILIANO
Issued by: Namirial CA Firma Qualificata
Signing time: 04-04-2023 14:26:39
IP address: 212.60.12.59

Namirial S.p.A.
Via Caduti sul Lavoro n. 4, 60019 Senigallia (An) - Italia | Tel. +39 071 63494
www.namirial.com | amm.namirial@sicurezzapostale.it | P.IVA IT02046570426
C.F. e iscriz. al Reg. Impr. Ancona N. 02046570426 | REA N. AN - 157295
Codice destinatario T04ZHR3 | Capitale sociale € 7.762.625,20i.v.

Indice

Storia delle modifiche 9
Riferimenti tecnici e normativi 14
Definizioni ed acronimi 18
Tabella di corrispondenza 22
Descrizione sintetica di Namirial S.p.A. 23
Contatti di Servizio e HelpDesk 25
1. Introduzione 26
1.1 Scopo e campo di applicazione 26
1.2 Nome e identificativo del documento 27
1.3 Partecipanti PKI e responsabilità 28
1.3.1 Certification Authority 28
1.4 Organizzazione del personale 29
1.4.1 Registration Authority 31
1.4.2 Local Registration Authority 31
1.4.3 Titolare 32
1.4.4 Richiedente 34
1.4.4.1 Terzo Interessato 34
1.4.5 Destinatario 35
1.5 Utilizzo del Certificato 35
2. Amministrazione del Manuale Operativo 36
2.1 Pubblicazione e archiviazione 36
2.1.1 Archiviazione 36
2.1.2 Pubblicazione dei Certificati 36
2.1.3 Frequenza di pubblicazione 36
2.1.4 Controllo degli accessi agli archivi pubblici 37
3. Identificazione ed Autenticazione (I&A) 38
3.1 Naming 38
3.1.1 Significato dei nomi 38
3.1.2 Regole di interpretazione dei tipi di nomi 38
3.1.3 Univocità dei nomi 39

3.1.4 Pseudonimia dei Richiedenti 39
3.1.5 Riconoscimento, autenticazione e ruolo dei marchi registrati 39
3.2 Convalida iniziale dell'identità 39
3.2.1 Documenti di riconoscimento accettati 40
3.3 Modalità di Autenticazione per Persone Fisiche 41
3.3.1 Riconoscimento De Visu 42
3.3.2 Identificazione mediante LiveID+ 44
3.3.3 Identificazione mediante procedura self 44
3.3.4 Identificazione mediante Certificato di Firma Qualificata 45
3.3.5 Identificazione mediante Strumenti di Autenticazione Elettronica 45
3.3.6 Identificazione mediante processi conformi alla Normativa PSD2 46
3.3.7 Soluzioni certificate da AgID 47
3.4 Certificati Qualificati per Persone Giuridiche 47
3.5 Identificazione ed Autenticazione per il rinnovo delle chiavi e dei Certificati 47
3.6 Identificazione ed Autenticazione per la richiesta di sospensione e revoca 48
4. Requisiti operativi del ciclo di vita dei Certificati 49
4.1 Soggetti che possono richiedere il rilascio di un Certificato 49
4.1.1 Richiesta del Certificato 50
4.2 Registrazione degli utenti 50
4.3 Processo di registrazione 50
4.4 Elaborazione della richiesta 51
4.5 Emissione del Certificato 52
4.6 Procedura di generazione delle chiavi 52
4.7 Accettazione del Certificato 52
4.8 Coppia di chiavi e utilizzo del Certificato 52
4.9 Modalità di consegna dei dispositivi di firma personali e dei codici segreti 53
4.9.1 Modifica dei codici del Titolare 53
4.9.1.1 Modifica PIN 53
4.10 Limitazioni d'uso 53
4.11 Rinnovo del Certificato 54
4.12 Modifica del Certificato 54

4.13 Revoca e sospensione del Certificato Qualificato 54
4.13.1 Motivi per la revoca o sospensione del Certificato 55
4.13.2 Sospensione in emergenza 56
4.13.3 Modalità per l'inoltro delle richieste 56
4.13.4 Tempi per la gestione delle richieste 57
4.13.5 Comunicazione dell'avvenuta revoca o sospensione 57
4.14 Servizio di verifica dello stato del Certificato 57
4.15 Modalità di sostituzione delle chiavi 57
4.15.1 Sostituzione delle chiavi di sottoscrizione degli utenti 57
4.15.2 Sostituzione delle chiavi di Marcatura Temporale 58
4.15.3 Sostituzione delle chiavi di certificazione 58
4.16 Risoluzione della sottoscrizione 59
4.17 Key escrow e recupero delle chiavi 59
5. Controlli e misure di sicurezza 60
5.1 Controlli fisici 60
5.1.1 Collocazione del sito 60
5.1.2 Accessi fisici 60
5.1.3 Energia elettrica e condizionamento 60
5.1.4 Esposizione all'acqua 61
5.1.5 Prevenzione degli incendi 61
5.1.6 Media storage 61
5.2 Controlli procedurali 61
5.2.1 Trusted roles 61
5.2.2 Numero delle persone coinvolte nelle attività 61
5.2.3 Identificazione ed autenticazione per ciascun ruolo 62
5.2.4 Attività che richiedono il dual control 62
5.3 Controlli sul personale 62
5.3.1 Qualifiche, esperienza e requisiti di autorizzazione 62
5.3.2 Check delle esperienze pregresse 63
5.3.3 Requisiti di formazione 63
5.3.4 Frequenza di aggiornamento della formazione e requisiti 63

5.3.5 Frequenza della job rotation 63
5.3.6 Sanzioni in caso di azioni non autorizzate 63
5.3.7 Requisiti del personale non dipendente 63
5.3.8 Documentazione fornita al personale 63
5.4 Procedure di gestione del giornale di controllo 64
5.4.1 Frequenza di salvataggio del giornale di controllo 64
5.4.2 Conservazione delle registrazioni del giornale di controllo 64
5.4.3 Backup del giornale di controllo 64
5.5 Archiviazione dei record 64
5.6 Sostituzione della chiave 65
5.7 Compromissione della chiave e disaster recovery 65
5.8 Piano di cessazione 65
6. Controlli di sicurezza tecnica 66
6.1 Generazione della coppia di chiavi 66
6.2 Modalità di generazione delle chiavi 66
6.2 Modalità di generazione delle chiavi di certificazione 67
6.2.1 Modalità di generazione delle chiavi di sottoscrizione degli utenti 67
6.2.1.1 Chiavi generate dal Certificatore 67
6.2.1.2 Chiavi generate dal Richiedente 68
6.2.3 Modalità di generazione delle chiavi di Marcatura Temporale 68
6.2.4 Consegna della chiave privata al Richiedente 69
6.3 Protezione della chiave privata e controlli ingegneristici sul modulo crittografico 69
6.3.1 Algoritmi crittografici e lunghezza delle chiavi 69
6.3.2 Funzioni di HASH 69
6.4 Altri aspetti relativi alla gestione della coppia di chiavi 69
6.5 Dati di attivazione 70
6.6 Controlli di sicurezza informatica 70
6.7 Controlli di sicurezza sul ciclo di vita del processo 70
6.7.1 Controlli sugli asset 70
6.7.2 Controlli sulla chiave privata 71
6.8 Controlli di network security 71

6.9 Timestamping 72
7. Policy, limiti d'uso e gestione dei Certificati 73
7.1 Profili dei Certificati 73
7.1.1 Namirial EU Qualified e-Signature 74
7.1.2 Namirial Firma Qualificata 75
7.1.3 Namirial CA Firma Qualificata 75
7.1.4 Namirial EU Qualified CA 76
7.2 Registro dei Certificati 77
7.3 Profilo CRL 77
7.4 Profilo OCSP 78
7.5 Accesso al registro dei Certificati 79
7.6 Gestione del registro dei Certificati 79
7.7 Archiviazione dei Certificati Qualificati e di Marcatura Temporale 79
8. Audit e conformità 80
8.1 Frequenza e circostanze della valutazione di conformità 80
8.2 Identità e qualifica di chi effettua il controllo 80
8.3 Rapporti tra Namirial e organismo di certificazione 80
8.4 Perimetro oggetto di valutazione 80
8.5 Azioni derivanti da non conformità 80
8.6 Comunicazione dei risultati 81
9. Altri aspetti legali e di business 82
9.1 Tariffe 82
9.2 Responsabilità finanziaria 82
9.3 Responsabilità del Titolare 82
9.4 Responsabilità della CA e limitazioni agli indennizzi 82
9.4.1 Limitazioni di responsabilità del Certificatore 82
9.4.1.1. Limitazioni e Indennizzi 83
9.5 Confidenzialità e trattamento dei dati personali 83
9.5.1 Protezione dei dati personali 83
9.5.2 Tutela e diritti degli interessati 83
9.5.3 Modalità del trattamento 84

9.5.4 Finalità del trattamento 84
9.5.5 Altre forme di utilizzo dei dati 84
9.5.6 Sicurezza dei dati 84
9.6 Archivi contenenti dati personali 85
9.7 Diritti di proprietà intellettuale 85
9.8 Obblighi e garanzie 85
9.8.1 Certification Authority 85
9.8.2 Registration Authority 86
9.8.3 Richiedenti o Titolari 86
9.8.4 Utenti finali 86
9.9 Limitazioni di garanzia 86
9.10 Limitazioni di indennizzo 86
9.11 Indennizzi 86
9.12 Termini e risoluzione 87
9.13 Comunicazioni 87
9.14 Procedure di risoluzione delle controversie 87
9.15 Foro competente 87
9.16 Legge applicabile 87
Appendice A: Strumenti e modalità per l'apposizione e la verifica della firma digitale 88
Firma con dispositivo di firma personale 88
Firma con applicazioni di firma automatica 89
Firma con applicazioni di firma remota 90
Modalità per l'apposizione e la definizione del Riferimento Temporale 91
Archiviazione e validità delle Marche Temporali 92
Precisone del Riferimento Temporale 92
Appendice B – Namirial Certificate Policy 93
Certificate Policies 93
QCP-l-qscd Policy for EU qualified certificate issued to a legal person where the private key related to the certificated public key resides in a QSCD 94
QCP-l Policy for EU qualified certificate issued to a legal person 96

QCP-n-qscd Policy for EU qualified certificate issued to a natural person where the private key related to the certificated public key resides in a QSCD (smart card or hsm) 98

QCP-n-qscd Policy for EU qualified certificate issued to a natural person where the private key related to the certificated public key resides in a QSCD (smart card or hsm) with etsi en 319 412-2 type 'B' or TYPE 'D' OR type 'f' key usage 101

QCP-n-qscd-A - Policy for EU qualified certificate issued to a natural person (retail) where the private key related to the certificated public key resides in a QSCD for automatic signature 104

QCP-n-qscd-D - Policy for EU qualified certificate issued to a natural person (retail) where the private key related to the certificated public key resides in a QSCD for disposable signature 107

QCP-n-qscd-LD - Policy for EU qualified certificate issued to a natural person (retail) where the private key related to the certificated public key resides in a QSCD for Long-Lived disposable signature 109

Appendice C: macro e comandi 113

Storia delle modifiche

VERSIONE	3.2
Data	26/02/2023
Motivazione	Aggiornamento
Modifiche	Revisione complessiva, aggiornamento in funzione della variazione del data center primario

VERSIONE	3.1
Data	17/10/2022
Motivazione	Aggiornamento
Modifiche	Variazione informazioni assistenza

VERSIONE	3
Data	19/05/2022
Motivazione	Aggiornamento
Modifiche	Revisione in tutti i paragrafi, accorpamento con il documento Certification Practice Statement

VERSIONE	2.5
Data	24/04/2020
Motivazione	Aggiornamento
Modifiche	Estensione della sezione definizioni; Aggiornamento della sezione certificazioni; Estensione degli obblighi per la LRA; Estensione modalità di riconoscimento;

VERSIONE	2.4
Data	14/06/2018
Motivazione	Revisione
Modifiche	Revisione del documento per adeguamento al Reg. (UE) 679/2016 §6.1 Aggiornato il DPO §6.2 Aggiornati i diritti degli interessati

VERSIONE	2.3
Data	30/06/2017
Motivazione	Aggiornamento
Modifiche	- Inserimento nuova CA per rilascio Certificati Qualificati per Firma elettronica e Sigillo Elettronico

VERSIONE	2.2
Data	30/05/2017
Motivazione	Aggiornamento
Modifiche	- Inserimento rilascio Certificati Qualificati per Sigillo Elettronico

VERSIONE	2.1
Data	23/05/2017
Motivazione	Aggiornamento
Modifiche	- Inserimento modalità di rilascio busta cartacea con Certificati attivi

VERSIONE	2.0
Data	12/12/2016
Motivazione	Aggiornamento
Modifiche	Inserimento della modalità di rilascio self-enroll con identificazione presso IR e dispositivo fornito dal Certificatore

VERSIONE	1.9.1
Data	08/07/2016
Motivazione	Aggiornamento
Modifiche	Aggiornamento OID Timestamp Authority

VERSIONE	1.9
Data	15/06/2016
Motivazione	Aggiornamento
Modifiche	Aggiornamento in seguito al recepimento del regolamento eIDAS

VERSIONE	1.8
Data	08/10/2015
Motivazione	Aggiornamento
Modifiche	Aggiornamento circa le modalità di identificazione e registrazione dell'utente.

VERSIONE	1.7
Data	01/07/2014
Motivazione	Aggiornamento
Modifiche	Aggiornamento ai Limiti d'uso e Certificate Policies. Aggiunte tipologie di firma. Modificata la procedura di rinnovo Certificati. Correzione di alcuni refusi all'interno del documento. Modificata la procedura di modalità di consegna dei dispositivi di firma personali e dei codici segreti e la modalità di visualizzazione della busta cieca digitale.

VERSIONE	1.6
Data	31/10/2013
Motivazione	Aggiornamento
Modifiche	Sostituzione riferimenti articoli DPCM 30/03/2009 con DPCM 22/02/2013. Aggiornamento agli obblighi delle LRA (§ 3.4). Aggiornamento policy Certificati (§ 4.1). Aggiornamento alla procedura per la visualizzazione della busta cieca digitale (§ 5.4.7.1). Aggiornamento della procedura di identificazione via webcam (§ 5.2.1).

VERSIONE	1.5
Data	01.10.2013
Motivazione	Aggiornamento
Modifiche	Rivisitazione generale del documento. Introduzione delle procedure operative per la firma automatica/remota. Modifica della procedura di rinnovo.

	Introduzione del riconoscimento via webcam.

VERSIONE	1.4
Data	20.02.2013
Motivazione	Aggiornamento
Modifiche	Cap. 1 Versioni e Riferimenti Cap. 2 Generalità. Cap. 13 Modalità di identificazione e registrazione dell'utente. Cap. 17 Modalità di consegna della busta cieca. Cap. 26 Macro e Comandi.

VERSIONE	1.3
Data	07.03.2011
Motivazione	Aggiornamento
Modifiche	Cap. 21 Modalità operative per l'utilizzo del software di verifica delle firme. Cap. 22 Modalità operative per la generazione della firma digitale. Cap. 19 Registro dei Certificati.

VERSIONE	1.2
Data	10.01.2011
Motivazione	Aggiornamento
Modifiche	Cap. 21 Modalità operative per l'utilizzo del software di verifica delle firme.

VERSIONE	1.1
Data	08.10.2010
Motivazione	Specificata la durata massima del Certificato Qualificato.
Modifiche	Capitolo 17.1 Rinnovo del Certificato qualificato

VERSIONE	1.0
Data	23.08.2010
Motivazione	Prima stesura

Modifiche	-

Riferimenti tecnici e normativi

Il Certificatore, nell'erogazione dei suoi servizi, è conforme alle normative e regolamenti europei e nazionali applicabili al momento dell'emissione. Tutti i regolamenti e le leggi applicabili sono riportati nella seguente tabella ed al personale del Certificatore.

NUM.	NORMATIVA	DESCRIZIONE
[I]	D.Lgs. 4/4/2006 n. 159	Decreto Legislativo 4 aprile 2006 n. 159 Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale.
[II]	DPCM 12/10/2007	Decreto del Presidente del Consiglio dei Ministri 12 ottobre 2007 Differimento del termine che autorizza l'autodichiarazione circa la rispondenza ai requisiti di sicurezza di cui all'art. 13, comma 4, del DPCM", pubblicato sulla GU 30 ottobre 2003, n. 13
[III]	D.Lgs. 82/2005	Decreto Legislativo 7 marzo 2005, n. 82 Codice dell'Amministrazione Digitale (CAD), con le modifiche ed integrazioni stabilite dal decreto legislativo 26 agosto 2016, n. 179.
[IV]	CNIPA/CR/48	Circolare CNIPA 6 settembre 2005 Modalità per presentare la domanda di iscrizione nell'elenco pubblico dei Certificatori di cui all'articolo 28, comma 1, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.
[V]	DPCM 22/02/2013	Decreto del Presidente del Consiglio dei Ministri 22 Febbraio 2013. Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali.
[VI]	REGOLAMENTO (UE) 2016/679	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 e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
[VII]	DPR 445/2000	Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
[VIII]	CNIPA 45/2009	CNIPA Deliberazione n. 45 del 21 maggio 2009 e successive modificazioni.

NUM.	NORMATIVA	DESCRIZIONE
		La presente deliberazione ha abrogato: Deliberazione CNIPA 17 febbraio 2005 n. 4 Deliberazione CNIPA 18 maggio 2006 n. 34 Regole per il riconoscimento e la verifica del documento informatico.
[IX]	CNIPA Limiti d'uso nei CQ	Limiti d'uso garantiti agli utenti ai sensi dell'articolo 12, comma 6, lettera c) della Deliberazione CNIPA 21 maggio 2009, n. 45
[X]	Direttiva UE 2015/2366	Direttiva (UE) 2015/2366 del Parlamento Europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE
[XI]	RFC 3647	Certificate Policy and Certification Practices Framework
[XII]	RFC 5280	Internet X.509 Public Key Infrastructure - Certificate and CRL Profile
[XIII]	ETSI TS 101 456	Policy requirements for Certification authorities issuing qualified certificates
[XIV]	ETSI TS 101 862	Qualified Certificate profile
[XV]	ETSI TS 102 023	Policy requirements for time-stamping authorities
[XVI]	ITU-T X.509 ISO/IEC 9594-8	Information Technology – Open Systems Interconnection – The Directory: Authentication Framework
[XVII]	DigitPA DC 69/2010	DigitPA - Determinazione Commissariale n. 69/2010 Modifica della Deliberazione 21 maggio2009 n. 45 del Centro Nazionale per l'Informatica nella pubblica Amministrazione, recante "Regole per il riconoscimento e la verifica del documento informatico", pubblicata il 3 dicembre 2009 sulla Gazzetta Ufficiale della Repubblica Italiana – serie generale – n. 282.
[XVIII]	CAD 30/12/2010 n.235	Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69.
[XIX]	D.Lgs. 231/2007	"Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attivita' criminose e di finanziamento del terrorismo nonche' della direttiva 2006/70/CE che ne reca misure di esecuzione".
[XX]	D. Lgs. 22 giugno 2012, n. 83	Misure urgenti per le infrastrutture l'edilizia ed i trasporti. art. 22 DigitPA e l'Agenzia per la diffusione delle tecnologie per l'innovazione sono soppressi. I due enti confluiscono nell' Agenzia per l'Italia Digitale.

NUM.	NORMATIVA	DESCRIZIONE
[XXI]	RFC 2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.
[XXII]	RFC 3161	Internet X.509 Public key infrastructure Time Stamp Protocol (TSP) PKIW Working Group IETF - Agosto 2001.
[XXIII]	DM 9/12/2004	Decreto del Ministero dell'Interno, del Ministro per l'innovazione e le tecnologie e del Ministro dell'economia e delle finanze 9 Dicembre 2004. Regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della Carta Nazionale dei Servizi" pubblicato nella Gazzetta Ufficiale n.296, 18 dicembre 2004.
[XXIV]	ETSI EN 319 401	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[XXV]	ETSI EN 319 421	Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
[XXVI]	ETSI EN 319 422	Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
[XXVII]	ETSI EN 319 411-1	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[XXVIII]	ETSI EN 319 411-2	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
[XXIX]	ETSI EN 319 411-3	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates
[XXX]	ETSI EN 319 412-1	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
[XXXI]	ETSI EN 319 412-2	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
[XXXII]	ETSI EN 319 412-3	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons

NUM.	NORMATIVA	DESCRIZIONE
[XXXIII]	ETSI EN 319 412-4	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates
[XXXIV]	ETSI EN 319 412-5	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
[XXXV]	ETSI TS 119 495	Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking
[XXXVI]	eIDAS n. 910/2014	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
[XXXVII]	QSCD	COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
[XXXVIII]	TSL	COMMISSION IMPLEMENTING DECISION (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
[XXXIX]	Electronic Signature Formats	COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

Tabella 1: Riferimenti tecnici e normativi

Definizioni ed acronimi

Sono qui riportati i significati di acronimi e di termini specifici, fatti salvi quelli di uso comune.

TERMINE O ACRONIMO	SIGNIFICATO
AgID	Agenzia per Italia Digitale.
Appartenenti all'Organizzazione	Dipendenti e/o associati a favore dei quali l'Organizzazione richiede l'emissione di un Certificato Qualificato (Es. Aziende, Enti, Associazioni di categoria, ecc.)
Autorità per la marcatura temporale [Time-stamping authority]	È il sistema software/hardware, gestito dal Certificatore, che eroga il servizio di marcatura temporale.
Certificato digitale, Certificato Qualificato	È un documento elettronico che attesta, con una firma digitale, l'associazione tra una chiave pubblica e l'identità di un soggetto (persona fisica).
Certificato disposable	Certificato di Firma Qualificata con intervallo di validità breve (eg. 30 giorni) e intervallo di utilizzo di 60 minuti
Certificatore [Certification Authority]	È l'ente, pubblico o privato, abilitato a rilasciare Certificati digitali tramite procedura di certificazione che segue standard internazionali e conforme alla normativa italiana ed europea in materia.
Chiave privata	È la chiave crittografica utilizzata in un sistema di crittografia asimmetrica; ogni chiave privata è associata ad una chiave pubblica, ed è solo in possesso dal Titolare che la utilizza per firmare digitalmente i documenti.
Chiave pubblica	È la chiave crittografica utilizzata in un sistema di crittografia asimmetrica; ogni chiave pubblica è associata ad una chiave privata, ed è utilizzata per verificare la firma digitale apposta su un documento informatico dal Titolare della chiave asimmetrica.
CIE	Carta d'Identità Elettronica, è il documento di identificazione destinato a sostituire la carta d'identità cartacea sul territorio italiano.
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione, l'Organismo di controllo istituito dal Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri.
CNS	Carta Nazionale dei Servizi

TERMINE O ACRONIMO	SIGNIFICATO
CRL – Lista di revoca e sospensione dei Certificati	È una lista di Certificati che sono stati resi "non validi" dal Certificatore prima della loro naturale scadenza. La revoca rende i Certificati "non validi" definitivamente. La sospensione rende i Certificati "non validi" per un tempo determinato.
CRS	Carta regionale dei servizi
CUC	È il Codice Univoco Certificato ed è indicato sulla Richiesta di Registrazione ed inserito nel Certificato. Identifica in modo univoco il Certificato emesso dal Certificatore.
CUT	È il Codice Univoco Titolare ed è indicato sulla Richiesta di Registrazione
Destinatario	È il soggetto a cui è destinato il documento e/o di una evidenza informatica firmata digitalmente.
Dispositivo Sicuro per la Creazione della Firma	Un dispositivo per la creazione di una Firma elettronica che soddisfi i requisiti di cui all'allegato II di eIDAS.
eIDAS	Il 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;
Giornale di controllo	Consiste nell'insieme delle registrazioni, effettuate automaticamente o manualmente, degli eventi previsti dalle Regole Tecniche di base.
IUT	Identificativo Univoco del Titolare, diverso per ogni Certificato emesso.
LDAP [Lightweight Directory Access Protocol]	È un protocollo standard per l'interrogazione e la modifica dei servizi di directory (segue gli standard X.500).
LRA	È la persona fisica o giuridica delegata dal Certificatore allo svolgimento delle operazioni di emissione dei Certificati, secondo le modalità individuate e descritte nel presente Manuale. L'ente deve aver preventivamente stipulato accordi di servizio con il Certificatore. L'LRA può avvalersi di RAO per le operazioni identificazione, registrazione ed emissione.
Marca Temporale [Timestamp]	È il riferimento temporale che consente la validazione temporale.
Manuale Operativo	È il documento pubblico depositato presso AgID che definisce le procedure applicate dal Certificatore nello svolgimento della propria attività.
OID [Object Identifier]	È una sequenza di numeri, registrata secondo lo standard ISO/IEC 6523, che identifica un determinato oggetto all'interno di una gerarchia.

TERMINE O ACRONIMO	SIGNIFICATO
OCSP [Online Certificate Status Protocol]	È un protocollo che consente di verificare la validità di un Certificato in tempo reale.
Organizzazione	È un gruppo organizzato di utenti (es. enti, aziende, società, ordini professionali, Associazioni, ecc.) che hanno stipulato accordi con il Certificatore per il rilascio di Certificati di firma digitale ai propri dipendenti e/o associati.
OTP	One-Time-Password. Codice numerico generato da un dispositivo fisico utilizzato per effettuare un'autenticazione a due fattori.
PIN [Personal Identification Number]	Codice associato ad un dispositivo sicuro di firma, utilizzato dal Titolare per accedere alle funzioni del dispositivo stesso
PSD2	Payment Services Directive relativa ai servizi di pagamento nel mercato interno
PUK	Codice personalizzato utilizzato dal Titolare per riattivare il proprio dispositivo in seguito al blocco dello stesso per errata digitazione del PIN.
RA	Registration Authority, soggetto che esegue l'identificazione dei Richiedenti dei Certificati Qualificati applicando le procedure definite dal Certificatore.
RAO	È soggetto espressamente delegato da Namirial allo svolgimento, per conto di quest'ultima, delle Operazioni di identificazione e registrazione del Titolare, nonché l'emissione dei Certificati. Tale soggetto deve appartenere ad una LRA.
Referente	È la persona fisica incaricata alla predisposizione di ogni documento necessario per il ciclo di vita della firma e che mantiene i contatti con il Certificatore.
Registro dei Certificati	È la lista dei Certificati emessi dal Certificatore, nella lista sono inclusi i Certificati revocati e sospesi, accessibile telematicamente.
Revoca del Certificato	È l'operazione con cui il Certificatore annulla la validità del Certificato, prima della sua naturale scadenza, da un dato momento, non retroattivo, in poi.
Richiedente	È il soggetto che richiede al Certificatore il rilascio di Certificati Qualificati. Se il Soggetto è diverso dal Titolare del Certificato l'identità del Richiedente verrà inserito nel campo Organization del Certificato X.509.
RSA	Algoritmo di crittografia asimmetrica, basato su chiavi pubbliche e private.

TERMINE O ACRONIMO	SIGNIFICATO
Servizio fiduciario	È un servizio elettronico definito nell'ambito del Regolamento eIDAS che può essere a) creazione, verifica e convalida di firme elettroniche, sigilli elettronici, validazioni temporali elettroniche, servizi elettronici di recapito Certificato; Certificati relativi a tali servizi; b) servizi di creazione, verifica e convalida dei Certificati di autenticazione di siti web; c) servizi di conservazione di firme; sigilli o certificati elettronici relativi a tali servizi
Servizio fiduciario qualificato	È un servizio fiduciario che soddisfa i requisiti stabiliti dal Regolamento eIDAS e ne fornisce le relative garanzie in termini di sicurezza e qualità.
SHA-256 [Secure Hash Algorithm]	Algoritmo di crittografia che genera una impronta digitale di 256 bit.
Sigillo	È un insieme di dati in forma elettronica acclusi, o connessi, tramite associazione logica, ad altri dati in forma elettronica, per garantirne la provenienza e l'integrità.
Sospensione del Certificato	È l'operazione con cui il Certificatore sospende la validità del Certificato, prima della sua naturale scadenza, per un periodo di tempo definito, non retroattivo.
Terzo Interessato	È la persona fisica o giuridica che dà il consenso, in conformità alle norme, al rilascio di Certificati Qualificati nei quali sia riportata l'appartenenza ad una Organizzazione ovvero eventuali poteri di rappresentanza o titoli e cariche rivestite. Ha il diritto/dovere di richiedere la revoca o sospensione del Certificato nel caso risultano modificati i requisiti in base ai quali lo stesso è stato rilasciato
Titolare	È il Firmatario, ovvero una persona fisica che crea una Firma elettronica
Token	È il dispositivo fisico (smart card, o chiave USB) che contiene la chiave privata del Titolare.
X.509	È uno standard ITU-T per le infrastrutture a chiave pubblica (PKI)

Tabella 2: Definizioni e Acronimi

Tabella di corrispondenza

La seguente tabella incrocia i temi previsti dal Art. 40, comma 3) del DPCM 22 febbraio 2013 con le corrispondenti sezioni del presente documento.

Art. 40, comma 3) del DPCM 22 febbraio 2013	Manuale Operativo
▪ dati identificativi del Certificatore	0
▪ dati identificativi della versione del manuale operativo	1.2
▪ responsabile del manuale operativo	1.2
▪ definizione degli obblighi del Certificatore, del Titolare e dei Richiedenti le informazioni per la verifica delle firme	1.4
▪ definizione delle responsabilità e delle eventuali limitazioni agli indennizzi	9.4
▪ indirizzo del sito web del Certificatore ove sono pubblicate le tariffe	1.3.1
▪ modalità di identificazione e registrazione degli utenti	3
▪ modalità di generazione delle chiavi per la creazione e la verifica della firma	4.6
▪ modalità di emissione dei Certificati	4.5
▪ modalità di inoltro delle richieste e della gestione di sospensione e revoca dei Certificati	4.13.3
▪ modalità di sostituzione delle chiavi	4.15
▪ modalità di gestione del registro dei Certificati	7.6
▪ modalità di accesso al registro dei Certificati	7.5
▪ modalità per l'apposizione e la definizione del riferimento temporale	Appendice A
▪ modalità di protezione dei dati personali	9.5.1
▪ modalità operative per l'utilizzo del sistema di verifica delle firme di cui all'art. 14, comma 1	Appendice A
▪ modalità operative per la generazione della firma elettronica qualificata e della firma digitale	Appendice A

Descrizione sintetica di Namirial S.p.A.

Namirial S.p.A. è una società di informatica e web engineering che ha trovato una propria specifica collocazione all'interno dell'Information Technology orientando la propria produzione di software verso le nuove e sempre più manifeste esigenze di adeguamento del sistema produttivo italiano ai nuovi scenari economici fortemente competitivi e globalizzati.

All'interno di una struttura economica nazionale caratterizzata per la gran parte dall'attività di piccole e medie realtà imprenditoriali si è ritenuto essenziale sviluppare soluzioni e servizi software accessibili anche sulla rete internet ed in grado di rispondere alle problematiche tecnologico-innovative emergenti in maniera professionale mantenendo una grande economicità di esercizio.

La società ha sede in una moderna struttura di oltre duemila metri quadrati, dove è operativo un *Internet Data Center, utilizzato come sito di Disaster Recovery,* dotato di tutti i sistemi di sicurezza necessari all'inviolabilità della struttura.

Namirial S.p.A. è:

Autorità di Certificazione Qualificata e accreditata dal 25/07/2016 presso AgID (ex DigitPA) ed è autorizzata all'emissione di Certificati Qualificati conformi al 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 Direttiva Europea 1999/93/CE, Certificati CNS e Marche Temporali.

Gestore di PEC, dal 26/02/2007, accreditato presso AgID (ex DigitPA) ed autorizzato alla gestione di **caselle** e **domini** di Posta Elettronica Certificata.

Gestore SPID, dal 13/04/2017, accreditato presso AgID (ex DigitPA) e Certificato (IT273825) ai sensi del:

- DPCM 24/10/2014;
- Regolamento di attuazione UE 2015/1502 della Commissione
- Regolamento (UE) 910/2014 eIDAS, art. 24

per la prestazione di servizi fiduciari di Identificazione Digitale.

Soggetto Conservatore, in conformità a:

- Regole Tecniche ai sensi dell'art. 71 del Codice dell'Amministrazione Digitale;
- Regolamento (UE) 910/2014 eIDAS, art. 24;

per la prestazione di servizi fiduciari di Conservazione a Norma.

Certificata ISO 9001. Namirial ha conseguito il Certificato n. 223776 rilasciato da **Bureau Veritas Italia S.p.A.**

Certificata ISO/IEC 27001. Namirial ha conseguito il Certificato n. IT280490 rilasciato da **Bureau Veritas Italia S.p.A.**

Certificata da Adobe. Da giugno 2013 Namirial è **membro dell'AATL** (Adobe Approved Trust List).

Namirial può inoltre vantare le acquisizioni strategiche di **Netheos**, azienda leader nel mercato francese specializzato in soluzioni per l'identificazione e l'onboarding digitale e di **Evicertia**, QTSP spagnolo affermato nella penisola iberica e in America Latina.
Entrambe le acquisizioni rafforzano il portafoglio di Namirial, così come la sua presenza sul mercato internazionale, determinando inoltre un ampliamento ed un improvement delle competenze dell'Azienda.

Contatti di Servizio e HelpDesk

Per ricevere informazioni sui servizi di Certificazione di Namirial S.p.A.sono disponibili i seguenti recapiti:

telefono: (+39) 071 63494
e-Mail: commercialeca@namirial.com
web: http://www.namirialtsp.com

Per ricevere informazioni tecniche ed assistenza sul servizio sono attivi i seguenti recapiti:

e-Mail: supportoca@namirial.com
web: http://www.namirialtsp.com

Il servizio è attivo nei giorni feriali con i seguenti orari:

dalle 9.00 alle 13.00 e dalle ore 15.00 alle 19

1. Introduzione

1.1 Scopo e campo di applicazione

Il presente documento rappresenta il **Manuale Operativo,** nonché la **Certificate Policy e Certification Practice Statement del servizio di certificazione digitale erogato da Namirial S.p.A,** ed ha come scopo la descrizione delle regole e delle procedure operative adottate da Namirial per tutte le attività inerenti all'emissione e alla gestione dei Certificati di Sottoscrizione Qualificati e delle marche temporali. All'interno del Manuale vengono inoltre descritte le procedure atte a garantire un adeguato livello di sicurezza e di affidabilità dei Certificati Qualificati in conformità con la normativa vigente alla data di emissione, così come le policy e le procedure relative al personale della Certification Authority deputato ad intervenire nel corso dell'intero ciclo di vita dei Certificati.
La struttura ed il contenuto di questo Manuale Operativo sono basate sul framework RFC 3647 standard.
Con l'entrata in vigore del Regolamento eIDAS non è più previsto per le Certification Authority un set documentale frammentato in Manuale Operativo, Certificate Policy e Certification Practice Statement: per questo motivo il Certificatore ha redatto un documento unico e funzionale agli scopi di informazione tecnica, consultazione e formazione cui il presente Manuale adempie in conformità al suddetto Regolamento.

La documentazione del Certificatore è organizzata secondo i principi dello standard ETSI EN 319 serie 400, nello specifico ETSI EN 319 411-1 "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates" from ETSI and ETSI EN 319 411-2 "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates" (disponibili all'indirizzo http://www.etsi.org). Viene dunque suddivisa nel seguente modo:

a) Il documento **NAMIRIAL Trust Services Practice Statement** descrive le procedure generali adottate dal Certificatore nell'erogazione dei servizi qualificati;
b) parti specifiche relative al servizio di certificazione (es. policy dei Certificati, procedure di identificazione, modalità operative del servizio specifico, etc.) sono descritte nel **Manuale Operativo** del servizio (il presente documento), in conformità alle norme nazionali;
c) parti specifiche relative al servizio di Marcatura Temporale sono descritte all'interno del presente Manuale.

La disciplina e le indicazioni contenute nel presente documento si applicano anche ai Certificati Qualificati di Firma Digitale emessi da Namirial per essere installati sulle CNS (Carta Nazionale dei Servizi) su richiesta delle Pubbliche Amministrazioni emittenti (Enti Emittenti). Per casi o soggetti particolari, per i quali si rendessero necessari

obblighi/regole e/o procedure operative specifiche, vengono rilasciati ulteriori documenti come "addendum".

1.2 Nome e identificativo del documento

Il presente documento denominato "NAMIRIAL-FDMT-MO" è identificato attraverso il livello di revisione e la data di rilascio presente su tutte le pagine. Nel preambolo del documento è inoltre riportato un paragrafo con la storia delle modifiche apportate.
Il Certificatore esegue, almeno una volta all'anno, un controllo di conformità del processo di erogazione del servizio di certificazione e, ove necessario, aggiorna questo documento anche in considerazione dell'evoluzione della normativa e standard tecnologici.
Il presente documento e gli eventuali ulteriori documenti rilasciati per soggetti e casi particolari, come *addendum* al Manuale Operativo, sono pubblicati dal Certificatore e da AgID e consultabili, per via telematica, al seguente indirizzo (ai sensi dell'art.40 comma 2 del DPCM 22 febbraio 2013)

http://support.namirial.com/it/
https://docs.namirialtsp.com/[1]

Tale URI è indicata nel campo *cSPuri* dell'estensione "Certificate Policies" dei Certificati Qualificati, dei server di Marcatura Temporale e OCSP.
Il documento è pubblicato in formato PDF firmato, in modo tale da assicurarne l'origine e l'integrità.
La responsabilità del presente Manuale Operativo è del Certificatore, nella figura del "Responsabile del servizio di certificazione e validazione temporale" (art. 40 comma 3 lettera c) del DPCM 22 febbraio 2013), il quale ne cura la stesura, la pubblicazione e l'aggiornamento.
Le comunicazioni riguardanti il presente documento possono essere inviate all'attenzione del suddetto responsabile contattabile mediante i seguenti recapiti:

E-mail: supportoca@namirial.com

Namirial S.p.A. garantisce la compliance dei propri Certificati con la Root ASN.1 OID indicata di seguito nel documento.

L'Object Identifier (OID) che identifica Namirial S.p.A. è iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1): 36023:

OID: 1.3.6.1.4.1.36203

[1] Il puntamento di questo indirizzo è http://support.namirial.com/it/

Tale OID è inserito nell'estensione CertificatePolicy dei Certificati, secondo le policies descritte nell'apposito paragrafo.

1.3 Partecipanti PKI e responsabilità

Gli attori indicati nel presente documento sono:

a) il Certificatore (**CA**)
b) la Registration Authority (**RA**)
c) la Local Registration Authority (**LRA**)
d) l'Operatore della Registration Authority (**RAO**)
e) il Titolare (Soggetto a cui è intestato il Certificato, **Subject**)
f) il Richiedente (Colui che sottopone la richiesta di certificazione alla CA ed assolve alle fasi di identificazione e registrazione, **Subscriber**)
g) il Destinatario (**Relying party**)
h) il Terzo Interessato
i) l'Incaricato alla Registrazione (**IR**)

1.3.1 Certification Authority

Namirial S.p.A. è **Certificatore Accreditato** (**Certification Authority**, CA) che emette, pubblica nel registro e revoca Certificati Qualificati di Sottoscrizione e CNS, in conformità alle regole tecniche vigenti.
La Certification Authority è una terza parte fiduciaria che firma i Certificati emessi dalla stessa con la propria chiave privata (CA key o chiave di root) e ne gestisce lo stato dei Certificati.
Il Certificatore è identificato come riportato nella seguente tabella.

Ragione Sociale:	**Namirial S.p.A.**
Sede Legale:	VIA CADUTI SUL LAVORO, 4 60019 - SENIGALLIA (AN) TEL: 071.63494 FAX: 071.60910
Sede di erogazione del servizio:	VIA CADUTI SUL LAVORO, 4 60019 - SENIGALLIA (AN) TEL: 071.63494 FAX: 071.60910
Partita IVA:	IT02046570426
Iscrizione registro delle imprese:	Ancona

REA:	02046570426
Capitale sociale:	7.762.625,20€ I.V.
Sito web del servizio:	http://www.namirialtsp.com
URL del Portale utente:	https://portal.namiriatsp.com
Sito web del Certificatore:	http://www.namirial.com
Email del servizio (PEC):	firmacerta@sicurezzapostale.it
Email del Certificatore:	supportoca@namirial.com

Tabella 3: Dati identificativi del Certificatore

1.4 Organizzazione del personale

Il personale preposto all'erogazione e controllo del servizio di certificazione è organizzato nel rispetto dell'art. 38 DPCM 22 febbraio 2013 In particolare, sono definite le seguenti figure organizzative:

- Responsabile della sicurezza
- Responsabile del servizio di certificazione e validazione temporale
- Responsabile della conduzione tecnica dei sistemi
- Responsabile dei servizi tecnici e logistici
- Responsabile delle verifiche e delle ispezioni (auditing)
- Responsabile della registrazione dei Titolari (RA) e dell'Help Desk;

Le responsabilità sopra descritte rientrano inoltre nei trusted roles previsti dallo standard ETSI EN 319-401, come descritto nell'apposito paragrafo.
Le figure sopra elencate possono avvalersi, per lo svolgimento delle attività di loro competenza, di addetti e collaboratori esterni.
Gli operatori di registrazione possono eventualmente operare anche presso sedi remote.
Al fine di ampliare le possibilità operative, le funzioni di registrazione possono essere svolte anche da terze parti, con sedi distribuite sul territorio, sulla base di appositi accordi stipulati con Namirial. In tal caso, tali terze parti ("Local Registration Authority", LRA) operano secondo quanto descritto dal presente documento e, per soggetti e/o casi particolari, dall'eventuale "addendum al manuale operativo" specifico.

Il Certificatore Namirial S.p.A:

- si attiene alla normativa vigente in materia di Firma Digitale e successive modificazioni ed al regolamento eIDAS n. 910/2014;
- provvede con certezza all'identificazione del Richiedente e del Titolare;
- si accerta dell'autenticità della richiesta di certificazione;
- specifica, nel Certificato Qualificato, ed eventualmente con il consenso del terzo interessato, i poteri di rappresentanza o altri titoli relativi all'attività professionale

o a cariche rivestite, previa verifica della documentazione presentata dal Richiedente che attesta la sussistenza degli stessi;

- richiede, quando previsto e prima di emettere il Certificato, la prova del possesso della chiave privata e verifica la correttezza della coppia di chiavi;
- rilascia e gestisce il Certificato Qualificato esclusivamente nei casi consentiti dal Titolare del Certificato nei modi o nei casi stabiliti nell'art. 32, comma 3, lettera b) del Dlgs 82/2005 (Codice dell'Amministrazione Digitale), nel rispetto del Regolamento UE 206/679 (GDPR), e successive modificazioni;
- fornisce o indica al Titolare i dispositivi sicuri di firma utilizzati nell'ambito del processo di rilascio del Certificato Qualificato per la generazione delle chiavi, la conservazione della chiave privata e le operazioni di firma, idonei a proteggere la chiave privata ed i dati per la creazione della firma del Titolare con criteri di sicurezza adeguati alla normativa vigente e alle conoscenze scientifiche e tecnologiche più recenti;
- informa il Titolare in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi, sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;
- non si rende depositario, nella loro interezza, dei dati per la creazione della firma del Titolare;
- non copia, né duplica, le chiavi private di firma del soggetto cui il Certificatore ha fornito il servizio di certificazione;
- procede alla tempestiva pubblicazione della revoca e della sospensione del Certificato Qualificato, nei seguenti casi:
    a) richiesta da parte del Titolare,
    b) richiesta del Terzo Interessato dal quale derivino i poteri di quest'ultimo,
    c) provvedimento dell'autorità,
    d) sospetti abusi o falsificazioni,

secondo quanto previsto dalle regole tecniche di cui al DPCM 22 febbraio 2013 e successive modifiche ed integrazioni;

- garantisce un servizio di revoca e sospensione dei Certificati sicuro e tempestivo nonché garantisce la pubblicazione affidabile, puntuale e sicura degli elenchi dei Certificati di firma sospesi e revocati, garantendo che non trascorrano più di 24 ore dalla richiesta di revoca o sospensione alla relativa pubblicazione;
- assicura la precisa determinazione della data e dell'ora di rilascio, scadenza, revoca e sospensione dei Certificati Qualificati;
- registra sul giornale di controllo, l'emissione dei Certificati Qualificati, con la specificazione della data e dell'ora di generazione; il momento di generazione del Certificato è attestato tramite riferimento temporale;
- tiene registrazione, anche elettronica, di tutte le informazioni relative al Certificato Qualificato dal momento della sua emissione almeno per 20 (venti) anni, anche al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;
- rende accessibile, per via telematica, la copia delle liste, sottoscritte da AgID, dei Certificati relativi alle chiavi di Certificazione di cui al DPCM 22 febbraio 2013
- utilizza sistemi affidabili per la gestione del registro dei Certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i Certificati siano

accessibili alla consultazione del pubblico soltanto nei casi consentiti dal Titolare;
- fornisce almeno un sistema che consenta al Titolare di effettuare la verifica della Firma Qualificata;
- nel caso di cessazione del servizio informa, almeno 60 (sessanta) giorni prima, i Titolari che tutti i Certificati non scaduti al momento della cessazione saranno revocati e a tempo debito provvede alla loro effettiva revoca ovvero indica gli estremi del Certificatore sostitutivo che si farà carico di detti Certificati;
- adotta le misure di sicurezza per il trattamento dei dati personali, ai sensi del Regolamento UE 206/679 (GDPR).

1.4.1 Registration Authority

La Registration Authority (RA) consiste nel soggetto deputato allo svolgimento delle seguenti attività:

1) identificazione del Titolare o del Richiedente
2) accettazione e validazione delle richieste relative all'emissione e alla gestione dei Certificati
3) registrazione dei Titolari e della relativa organizzazione
4) autorizzazione della CA all'emissione dei Certificati richiesti
5) erogazione del Certificato e conseguente notifica al cliente

La funzione di RA è svolta dagli impiegati Namirial autorizzati ad operare tramite conferimento di un mandato e successivamente al superamento di una specifica sessione formativa.

1.4.2 Local Registration Authority

La Local Registration Authority (LRA) è la persona fisica o giuridica, autorizzata dalla Certification Authority, responsabile delle attività relative all'emissione dei Certificati, in conformità con le procedure identificate e descritte in questo documento, previa sottoscrizione di un mandato contrattuale con la Certification Authority. La LRA può affidarsi ai propri Registration Authority Officers (RAO) per le operazioni di identificazione, registrazione ed emissione. La LRA svolge le stesse mansioni della RA, ma mediante soggetti esterni e distribuiti sul territorio.
Oltre ai RAO, la LRA può nominare, sempre tramite apposita contrattualistica, persone fisiche o giuridiche che svolgono esclusivamente l'attività di registrazione dei Titolari (Incaricati alla Registrazione IR).

La LRA per mezzo dei RAO è tenuta a:

- informare il Titolare in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti per accedervi, sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;
- informare il Titolare circa la modalità di firma e il tipo di Certificato ad esso connesso e la corretta custodia della credenziale di firma;

- informare il Titolare riguardo gli obblighi da quest'ultimo assunti in merito alla conservazione della credenziale di firma, con la massima diligenza, e separatamente dal dispositivo per l'apposizione della firma che contiene la chiave privata nel caso di Certificato emesso su dispositivo fisico;
- informare il Titolare riguardo agli obblighi da quest'ultimo assunti in merito a conservare con la massima diligenza il dispositivo OTP eventualmente fornito;
- richiedere, quando previsto e prima di rilasciare il Certificato, la prova del possesso della chiave privata e verificare la correttezza della coppia di chiavi;
- informare il Titolare delle misure di sicurezza adottate per il trattamento dei dati personali, ai sensi Regolamento UE 206/679 (GDPR);
- provvedere con certezza all'identificazione della persona che fa richiesta della certificazione;
- accertare l'autenticità della richiesta di certificazione;
- comunicare al Certificatore tutti i dati e documenti acquisiti durante l'identificazione del Titolare e previsti dalle procedure del Certificatore al fine di attivare tempestivamente la procedura di emissione del Certificato;
- verificare ed inoltrare al Certificatore le richieste di revoca/sospensione richieste dal Titolare presso LRA;
- attenersi scrupolosamente alle regole impartite dal Certificatore e presenti su questo documento;
- assicurarsi che il Richiedente e Titolare abbiano preso visione delle Condizioni Generali di contratto;
- consegnare al Richiedente e Titolare copia della documentazione di richiesta di emissione del Certificato dagli stessi sottoscritta.

Nei casi in cui la Local Registration Authority sia costituita presso uno tra i particolari organi della PA, quali ad esempio le Forze Armate e Forze dell'Ordine, su richiesta espressa della medesima, le attività e responsabilità di raccolta e archiviazione dei dati potranno essere gestite direttamente dalla LRA.
I RAO sono autorizzati ad operare dal Certificatore a seguito di adeguata formazione del personale addetto. Il Certificatore, salvo diritto di rivalsa, resta comunque l'unico ed il solo responsabile verso terzi dell'attività svolta dall'LRA.
Il Certificatore verifica periodicamente la rispondenza delle procedure adottate dalla LRA e dai suoi RAO e quanto indicato nel presente documento. In ogni caso, a semplice richiesta del Certificatore, la LRA è tenuta a trasmettere allo stesso tutta la documentazione in proprio possesso, relativa a ciascuna richiesta di emissione dei Certificati di sottoscrizione proveniente da ciascun Titolare.

1.4.3 Titolare

Il Titolare è l'entità identificata all'interno del Certificato come il possessore della chiave privata associata alla chiave pubblica consegnata all'interno del Certificato.

Il Titolare può essere:

- una persona fisica
- una persona fisica identificata in associazione ad una persona giuridica
- una persona giuridica (Organizzazione o una business unit o dipartimento identificato in associazione con un'Organizzazione

Il Titolare dei Certificati Qualificati è tenuto a:

- prendere visione del presente documento prima di richiedere il Certificato Qualificato e rispettarne le prescrizioni per quanto di propria competenza;
- fornire tutte le informazioni richieste dal Certificatore, garantendone l'attendibilità sotto la propria responsabilità;
- comunicare al Certificatore eventuali variazioni delle informazioni fornite all'atto della registrazione: dati anagrafici, residenza, recapiti telefonici, indirizzo di posta elettronica, ecc.;
- mantenere in modo esclusivo la conoscenza o la disponibilità dei dati per la creazione della firma (PIN, PUK e/o OTP) e il codice d'emergenza, conservandoli con la massima diligenza;
- mantenere separatamente il dispositivo che contiene la chiave privata dai dati di cui al punto precedente, al fine di garantirne l'integrità e la massima riservatezza, nel caso di Certificato emesso su dispositivo fisico;
- mantenere in modo esclusivo e conservare con la massima diligenza il dispositivo OTP eventualmente fornito;
- non utilizzare la Firma Qualificata per funzioni e finalità diverse da quelle per la quale è stata rilasciata;
- adottare le misure indicate nel presente manuale al fine di evitare di apporre Firme Qualificate su documenti contenenti macroistruzioni o codici eseguibili che ne modifichino gli atti o i fatti negli stessi rappresentati e che renderebbero, quindi, nulla l'efficacia della sottoscrizione;
- inoltrare, con le modalità indicate dal Certificatore, la richiesta di sospensione specificando la motivazione ed il periodo durante il quale la validità del Certificato deve essere sospesa;
- richiedere l'immediata sospensionedei Certificati Qualificati relativi alle chiavi contenute in dispositivi di firma di cui abbia perduto il possesso o difettosi, richiedendone la revoca una volta accertati gli eventi menzionati;
- inoltrare, con le modalità indicate dal Certificatore, la richiesta di revoca specificandone la motivazione e la sua decorrenza;
- sporgere denuncia, in caso di smarrimento o sottrazione del dispositivo di firma, alle autorità competenti;
- presentarsi presso l'LRA o dal Certificatore a seguito della richiesta di sospensione del Certificato per richiedere, ove del caso, la revoca dello stesso con l'apposito modulo;
- utilizzare esclusivamente dispositivi di firma indicati ovvero forniti dal Certificatore in modo conforme a quanto indicato nel presente manuale;
- adottare idonee misure di sicurezza (es. antivirus / antimalware) al fine di prevenire un utilizzo fraudolento dei dispositivi di firma.

1.4.4 Richiedente

Il Richiedente è una persona fisica o giuridica che richiede un Certificato. Questo può coincidere con il Titolare, oppure operare per conto di uno o più Titolari con i quali l'organizzazione è collegata (terzo interessato). Ad esempio, il Richiedente può coincidere con un'azienda che richiede i Certificati per i propri impiegati, perché intrattengano rapporti di business a nome dell'organizzazione.
A seconda se il Titolare del Certificato è una persona fisica piuttosto che giuridica, i rapporti tra Richiedente e Titolare debbono rientrare nelle seguenti casistiche.

Persona fisica
Al fine di richiedere un Certificato per una persona fisica, il Richiedente è:

- la stessa persona fisica;
- una persona fisica delegata a rappresentare il Titolare; (NOTA: disposizioni legislative locali possono indirizzare il passaggio di responsabilità a terzi). In questo caso, il Richiedente viene definito "Terzo interessato", nel Certificato vengono inserite le indicazioni della persona giuridica e/o il ruolo.
- una qualsiasi entità cui è associata la persona fisica (ad esempio l'organizzazione presso cui è assunta la persona fisica o una persona giuridica non-profit di cui è membro la persona fisica).

Persona giuridica
Al fine di richiedere un Certificato per una persona giuridica, il Richiedente è:

- Una qualsiasi entità legalmente riconosciuta a rappresentare la persona giuridica
- Un legale rappresentante o una persona giuridica con poteri di firma presso le proprie sussidiarie, dipartimenti o business unit.

Il Richiedente è tenuto a:

- provvedere, previo esplicito consenso dei Titolari, a raccogliere i dati necessari alla registrazione, nella forma richiesta dal Certificatore;
- chiedere la revoca e la sospensione dei Certificati, secondo le modalità indicate nel presente Documento, ogniqualvolta vengano meno i presupposti in base ai quali il Certificato è stato rilasciato al Titolare. (ad esempio, cessazione della propria attività, cambio mansioni, sospensioni, ecc.);
- comunicare tempestivamente al Certificatore ogni modifica delle circostanze indicate al momento del rilascio del Certificato rilevanti ai fini del suo utilizzo;
- inoltrare la richiesta di revoca o sospensione al Certificatore munita di sottoscrizione e della motivazione, con la specificazione della sua decorrenza.

1.4.4.1 Terzo Interessato
Il Terzo Interessato coincide con la società od organizzazione a cui risulta collegato il Titolare e che ha avanzato la richiesta del Certificato in sua vece.

In questo caso il Titolare viene individuato dal referente del Terzo Interessato che ha sottoscritto una convenzione con la CA.

1.4.5 Destinatario

Il Destinatario è una persona fisica o giuridica a cui è destinato il documento, il cui Certificato di firma apposto è verificabile tramite il riferimento di una chiave pubblica inserita all'interno del Certificato del Titolare. I Destinatari, al fine di verificare la validità di un Certificato, debbono sempre riferirsi alle informazioni di revoca della CA Namirial (CRL e OCSP).
I Destinatari debbono rispondere agli obblighi contenuti all'interno del presente documento.
Coloro che verificano le firme digitali generate con chiavi certificate da Namirial sono tenuti a verificare:

- che il Certificato del Titolare sia stato emesso da un Certificatore accreditato;
- l'autenticità del Certificato contenente la chiave pubblica del firmatario del documento;
- l'assenza del Certificato dalla Lista di Revoca e Sospensione (CRL) dei Certificati,
- la validità della firma tramite apposita applicazione,
- l'esistenza ed il rispetto di eventuali limitazioni all'uso del Certificato utilizzato dal Titolare;
- l'integrità del documento ricevuto, tramite un software di verifica conforme alla normativa vigente.

1.5 Utilizzo del Certificato

I Certificati emessi da Namirial sono validi al fine dell'applicazione di firme digitali su documenti informatici opponibili a terzi.
È proibito qualsiasi utilizzo improprio dei Certificati emessi da Namirial, secondo le disposizioni contenute in questo documento e all'interno del PKI Disclosure Statement.
Namirial si riserva la possibilità di revocare immediatamente qualsiasi Certificato utilizzato in maniera impropria di cui entri a conoscenza.
Si presuppongono la competenza e la conoscenza adeguate e necessarie per l'utilizzo corretto del Certificato.

2. Amministrazione del Manuale Operativo

Il presente documento è definito, pubblicato ed aggiornato da Namirial. Ogni modifica di questo documento è sottoposta ad un processo di verifica interno, approvata dall'alta direzione e notificata all'Agenzia per l'Italia Digitale (AgID). Domande, osservazioni o reclami in ordine al presente Manuale Operativo debbono essere rivolte via mail all'indirizzo: supportoca@namirial.com o via posta elettronica certificata a firmacerta@sicurezzapostale.it.
Namirial S.p.A. aggiorna periodicamente la propria documentazione pubblica disponibile al sito internet dell'organizzazione.

2.1 Pubblicazione e archiviazione

2.1.1 Archiviazione

Il repository Namirial è disponibile agli indirizzi

https://docs.namirialtsp.com/
http://support.namirial.com

La CA gestisce il repository in maniera indipendente e ne è direttamente responsabile.

2.1.2 Pubblicazione dei Certificati

La CA pubblica i seguenti documenti nel proprio sito web:

- Trust Service Practice Statement (TSPS)
- Certification Practice Statement (CPS) e Certificate Policy (CP), integrate nel presente Manuale Operativo (MO)
- Certificati CA di root

Namirial S.p.A. opera in conformità alla versione corrente dei "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" ivi pubblicati: http://www.cabforum.org.
In caso di incongruenza tra il presente documento e i Requirements, questi ultimi saranno predominanti.

2.1.3 Frequenza di pubblicazione

Questo documento ed i suoi allegati sono pubblicati sul sito della CA ogni qualvolta vengano aggiornati. Ad ogni major change viene sottoposto alla verifica da parte di AgID.

2.1.4 Controllo degli accessi agli archivi pubblici

Questo documento ed i suoi allegati sono disponibili pubblicamente ed accessibili solo in lettura.

3. Identificazione ed Autenticazione (I&A)

3.1 Naming

Namirial emette ogni Certificato in compliance con i seguenti Standard:

- ETSI EN 319 411-1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-2 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 412-1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
- ETSI EN 319 412-2 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
- ETSI EN 319 412-3 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
- ETSI EN 319 412-5 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

I Certificati di sottoscrizione riportano il valore “no repudiation” per l’estensione di utilizzo della chiave. Il campo “subject” nel Certificato contiene informazioni intellegibili che permettono l’identificazione del proprietario del Certificato (persona fisica o giuridica).
In caso di Certificati intestati a persone fisiche, il campo “soggetto” contiene, almeno:

- countryName;
- givenName and surname
- commonName
- DNQualifier
- SerialNumber

In caso di Certificati di persona giuridica, il campo “soggetto” contiene, almeno:

- countryName;
- organization Name
- organizationIdentifier
- commonName

3.1.1 Significato dei nomi

L’attributo del Certificato Distinguished Name (DN) identifica in maniera univoca il soggetto a cui è rilasciato il Certificato.

3.1.2 Regole di interpretazione dei tipi di nomi

Namirial si attiene allo standard X500.

3.1.3 Univocità dei nomi

Persona fisica

Nel Certificato vengono indicati nome, cognome ed un codice identificativo a garanzia dell'univocità del Soggetto. Per i cittadini italiani, il codice univoco del soggetto è rappresentato dal codice fiscale, mentre per i cittadini esteri può essere definito un codice univoco tratto dal documento di riconoscimento presentato durante la fase di identificazione.

Pertanto, in assenza di codice fiscale o attributo equivalente, in caso di Certificato il cui Richiedente sia estero, all'interno del Certificato potrà essere indicato:

- un codice identificativo tratto da un documento di identità valido, utilizzato nella procedura di riconoscimento
- un identificativo univoco determinato dalla CA e codificato in base 64

Per i Richiedenti italiani deve essere specificato il codice fiscale in quanto utilizzato dalle Pubbliche Amministrazioni come identificativo del cittadino.

Persona giuridica

Nel caso di persona giuridica, nel Certificato vengono riportati la ragione sociale, il codice fiscale e la partita iva.

Se il Richiedente è una pubblica amministrazione, quindi entità sprovvista di partita iva, viene indicato il codice IPA.

3.1.4 Pseudonimia dei Richiedenti

Le procedure Namirial contemplano la possibilità di inserire uno pseudonimo per il Richiedente, su richiesta specifica dello stesso.

3.1.5 Riconoscimento, autenticazione e ruolo dei marchi registrati

Si specifica che all'interno del Certificato di Sigillo, nel campo commonName è consentito al Richiedente inserire un testo libero, qualora intenda specificare una nomenclatura differente rispetto alla ragione sociale (es. marchio).

Il Richiedente, in fase di inserimento, si assume la responsabilità in merito al popolamento di tale campo, in quanto la CA non effettua verifiche sull'alternativa inserita.

3.2 Convalida iniziale dell'identità

Il processo di validazione dell'identità comporta la verifica da parte di Namirial dell'identità del Richiedente e dell'identità del Titolare nel caso in cui questa sia diversa dalla prima (ad esempio, il Titolare sta agendo per conto di uno o più Titolari distinti a cui è collegato). Namirial chiederà alle due parti di fornire informazioni sull'identità e

documenti di supporto per eseguire l'identificazione. Le procedure per rilasciare un Certificato Qualificato sono:

- Registrazione
- Identificazione

Gli operatori della Registration Authority o di un ufficio delegato conducono la registrazione e l'identificazione, sotto il controllo e la responsabilità di Namirial.
Il processo delegato può essere condotto da:

- Operatori Namirial
- Dall'entità cui Namirial delega le proprie attività di identificazione

L'identificazione si basa su documenti validi sul territorio locale, come un documento di riconoscimento valido. Namirial conserva i documenti di identificazione o attestati emessi da una fonte appropriata e autorizzata, e conserva queste informazioni per il periodo richiesto dalla normativa (20 anni).

3.2.1 Documenti di riconoscimento accettati

Il Titolare o Richiedente possono identificarsi per mezzo di un documento d'identità o un documento di riconoscimento equipollente ai sensi dell'art.35 del DPR 445/2000 in corso di validità. A titolo esemplificativo si riporta una lista di documenti che possono essere presentati da cittadini italiani, purché siano muniti di fotografia del Titolare, firma autografa del Titolare e di timbro e rilasciati da un'Amministrazione dello Stato:

- Carta d'identità,
- Passaporto,
- Patente di guida,
- Permesso di UMB con fotografia.

In caso di Local Registration Authority operanti a livello internazionale o cittadini stranieri che richiedano un Certificato in Italia, i documenti che possono essere presentati sono consultabili all'interno del database PRADO (https://www.consilium.europa.eu/prado/en/prado-start-page.html).
È facoltà del soggetto che effettua l'identificazione escludere l'ammissibilità del documento utilizzato dal Titolare se ritenuto non rispondente ai requisiti indicati.
Per garantire la tutela e la gestione dei propri dati personali in piena aderenza al Regolamento (UE) 2016/679 (GDPR), ad ogni Richiedente verrà preventivamente fornita l'informativa sulla privacy e, nel caso di identificazione tramite sistema di videoriconoscimento, richiesto il consenso alla registrazione ed al trattamento dei dati da parte degli incaricati del Certificatore.

3.3 Modalità di Autenticazione per Persone Fisiche

L'identità del Titolare può essere accertata mediante le seguenti modalità ed in conformità con l'art. 24 del Regolamento eIDAS.

Modalità	Soggetti abilitati ad eseguire l'identificazione	Condizioni tecnologiche di autenticazione richieste per l'identificazione
De visu	Certification Authority (CA) Registration Authority (RA) Local Registration Authority (LRA) Incaricato alla Registrazione (IR)	Nessuna
LiveID	Certification Authority (CA) Registration Authority (RA) Local Registration Authority (LRA) Incaricato alla Registrazione (IR)	Nessuna
FEQ	Certification Authority (CA) Registration Authority (RA) Local Registration Authority (LRA) Incaricato alla Registrazione (IR)	Firma elettronica qualificata emessa da un QTSP
SPID/CIE	Certification Authority (CA) Registration Authority (RA) Local Registration Authority (LRA) Incaricato alla Registrazione (IR)	Utilizzo di un mezzo di identificazione elettronica preesistente (identità digitale SPID o CIE)
Identificazione elettronica nazionale	Certification Authority (CA) Registration Authority (RA) Local Registration Authority (LRA)	Utilizzo di un mezzo di identificazione elettronica nazionale preesistente, notificato dallo Stato Membro
Processi AML	Titolari destinatari degli obblighi Antiriciclaggio ai sensi delle normative di recepimento della Direttiva 2005/60/CE del Parlamento Europeo e	Processo di autenticazione autorizzato AgID

	del Consiglio relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, e delle successive normative comunitarie di esecuzione e s.m.i. (Normativa PSD2)	

3.3.1 Riconoscimento De Visu

Identificazione da parte di un RAO

Nel caso di rilascio di Certificati Qualificati a persone fisiche, se il Titolare coincide con il Richiedente, lo stesso può essere identificato "de visu". La modalità di riconoscimento de visu prevede la presenza fisica contemporanea del Titolare e dell'operatore abilitato ad eseguire il riconoscimento, che può corrispondere a:

- personale autorizzato del Certificatore o dagli uffici di registrazione LRA, tramite i RAO;
- un pubblico ufficiale;
- un incaricato alla registrazione (IR).

Nel caso in cui il Titolare non coincida con il Richiedente, viene coinvolta la figura del Terzo Interessato, ovvero della società od organizzazione a cui risulta collegato il Titolare e che fa le veci del Richiedente.

Identificazione da parte di un Pubblico Ufficiale

Il Richiedente, qualora coincida con il Titolare, compila la richiesta di emissione di Certificati e la dichiarazione sostitutiva dell'atto di notorietà (scaricando il modulo dalla sezione "*Documenti*" del sito https://support.namirial.com/), si reca presso un Pubblico Ufficiale e sottoscrive la richiesta e la dichiarazione facendo autenticare le proprie firme autografe, ai sensi della normativa che disciplina le loro attività e da quanto indicato nel D.L. 3 Maggio 1991 n. 143 e successive modifiche ed integrazioni.

Identificazione da parte di un RAO tramite app IDCheck

Anche in tale modalità l'identificazione è effettuata da parte di un RAO, che procederà utilizzando l'app Namirial IDCheck, sviluppata secondo le linee guida OWASP[2]. L'applicazione è disponibile soltanto previa emissione di un voucher e solo ai RAO che hanno completato con successo il percorso formativo obbligatorio.

[2] La top 10 OWASP (Open Web Application Security Project) è un documento di linee guida di sviluppo sicuro in ambiente web.

Durante tale processo, il RAO acquisisce il documento di riconoscimento e il codice fiscale, presente sulla tessera sanitaria, mediante l'app che effettua una lettura dei dati in essi contenuti sfruttando la tecnologia OCR. L'app vincola, inoltre, il Richiedente ad essere riconosciuto previa acquisizione di una fotografia, che viene scattata dal RAO. L'app effettua poi un face match tra tali acquisizioni e la fotografia presente all'interno del documento di riconoscimento.
Nel caso in cui l'esito del riconoscimento sia positivo, il RAO può procedere con l'emissione dei Certificati. Diversamente, dovrà effettuare un nuovo riconoscimento.

Identificazione da parte di un soggetto Incaricato alla Registrazione
In tale modalità l'identificazione è effettuata da un soggetto denominato Incaricato alla Registrazione (IR) appartenente ad una società terza, ed è prevista la presenza fisica del Richiedente (che deve coincidere con il Titolare del Certificato) dinnanzi al suddetto incaricato. Tali soggetti (gli IR) possono operare successivamente alla stipula di un contratto tra il Certificatore e la Società Terza. Quest'ultima indica il proprio operatore, che viene individuato con tale ruolo e che deve agire secondo le procedure stabilite e contenute nel presente Manuale Operativo per quanto concerne le fasi di identificazione, registrazione dei dati del Richiedente, verifica della corretta compilazione del Modulo di Registrazione e Richiesta del Certificato, dell'apposizione della firma autografa sul contratto e, quando previsto, consegna "brevi manu" del dispositivo.
Il Richiedente deve presentarsi all'IR esibendo:

- il Modulo di Registrazione e Richiesta del Certificato contenente i dati anagrafici del Richiedente;
- il Documento di Riconoscimento rispondente a quelli previsti al paragrafo 3.2.1
- le condizioni generali di contratto;
- l'informativa sulla privacy;

Per l'identificazione, l'IR può verificare l'identità del Richiedente verificandone il riscontro con un documento di riconoscimento in corso di validità, verificando che, nel caso di pre-registrazione via Web, il Documento sia lo stesso già caricato in procedura e deve astenersi dall'accettare qualsiasi altro modulo che non sia quello emesso dal Certificatore.
Il Modulo di Registrazione e Richiesta del Certificato viene sottoscritto con firma autografa dal soggetto Richiedente dinnanzi all'IR.
Nel caso di utilizzo della busta cieca digitale, successivamente alla consegna del dispositivo, il Certificatore inoltra la busta all'indirizzo email fornito dal Titolare e sottoscritto al momento della consegna del dispositivo in presenza dell'IR.
Si rende noto in tal senso che il soggetto Richiedente, firmando il Modulo di Registrazione e Richiesta del Certificato, si assume gli obblighi di cui al paragrafo 9.8.3.
In ogni caso la responsabilità delle operazioni di registrazione, identificazione e validazione è del Certificatore.

Identificazione da parte di un referente del Terzo Interessato che ha sottoscritto una convenzione

Il Terzo Interessato, nella persona del Referente, raccoglie ed inoltra al Certificatore i seguenti documenti, opportunamente sottoscritti:

- modulo di richiesta emissione Certificato
- una copia di un documento d'identità o un documento di riconoscimento equipollente ai sensi dell'art.35 del DPR 445/2000 in corso di validità.

I suddetti documenti potranno essere firmati attraverso firma elettronica avanzata, qualificata o autografa.

3.3.2 Identificazione mediante LiveID+

L'identificazione mediante LiveID+ avviene stabilendo un contatto via web con un operatore autorizzato ad operare dalla CA, individuabile in un RAO o un IR.

All'avvio della sessione, ciascun Richiedente sarà informato circa il fatto che per ragioni di sicurezza la videochiamata (video/voce) sarà registrata e conservata in conformità a quanto indicato nell'art. 32, comma 3, lettera j) del CAD e che in caso di dichiarazioni mendaci, falsità negli atti, uso o esibizione di atti falsi o contenenti dati non più rispondenti a verità, sarà soggetto alle sanzioni penali previste ai sensi dall'art 76 del DPR 445/2000.

Solo dopo l'assenso del Richiedente potrà essere avviata la registrazione della video conferenza che inizierà con la ripetizione della procedura di richiesta del consenso.

Le specifiche procedure telematiche di identificazione e registrazione studiate dal Certificatore e attuate dai propri incaricati in tale sede, non sono rese pubbliche per ragioni di sicurezza.

In dettaglio, i dati di registrazione, costituiti da file audio video e metadati strutturati in formato elettronico, vengono conservati in forma protetta per una durata ventennale, presso il Certificatore. Tale procedura in uso soddisfa quanto richiesto dall'art. 32, comma 3, lettera a) del CAD.

3.3.3 Identificazione mediante procedura self

Un'altra modalità di video riconoscimento è rappresentata dall'identificazione con procedura self. Tale processo è stato sottoposto a verifica e certificazione da parte di un Conformity Assessment Body (CAB) accreditato dall'ente italiano di accreditamento Accredia.

Rispetto a quanto già descritto nel paragrafo precedente, l'utente sarà guidato dal sistema ad eseguire gli step che seguono, durante una sessione registrata previo consenso:

- Conferire il documento di riconoscimento ed un documento contenente un identificativo univoco (codice fiscale su tessera sanitaria per i riconoscimenti effettuati per cittadini italiani o equivalenti per cittadini di stati esteri);
- Riprendere il proprio volto;
- Eseguire azioni casuali.

La procedura effettuerà il face match per la verifica biometrica tra la ripresa e la foto del documento di riconoscimento. In ogni caso, un operatore di back office dovrà verificare le evidenze acquisite.
Qualora la verifica abbia successo, la Certification Authority è autorizzata ad emettere il Certificato e può procedere con il rilascio.
In caso negativo, il Richiedente dovrà eseguire nuovamente la procedura.

3.3.4 Identificazione mediante Certificato di Firma Qualificata

Questa modalità prevede che il Richiedente compili il modulo di richiesta previsto per il rilascio della firma digitale, che lo sottoscriva mediante Firma Elettronica Qualificata e che sottometta a sistema il documento firmato. Una procedura automatizzata effettua i seguenti controlli:

- Validità della firma;
- Coincidenza del firmatario del modulo con il Richiedente;
- Che una copia dello stesso documento di richiesta non sia già stata utilizzata per ottenere un altro Certificato di firma digitale.

3.3.5 Identificazione mediante Strumenti di Autenticazione Elettronica

Questa modalità prevede che il Richiedente sia in possesso di un mezzo di identificazione elettronica preesistente:

- Notificato dallo Stato Membro ai sensi dell'articolo 9 del Regolamento eIDAS, di livello elevato;
- Notificato dallo Stato Membro ai sensi dell'articolo 9 del Regolamento eIDAS, di livello significativo, a patto che fornisca una garanzia equivalente sotto il profilo dell'affidabilità alla presenza fisica;
- Non notificato ed emesso da una autorità pubblica o un soggetto privato, a condizione che fornisca una garanzia equivalente alla presenza fisica sotto il profilo dell'affidabilità, e questa sia confermata da un organismo di valutazione della conformità.

Nello specifico, relativamente allo Stato Italia vengono riconosciuti come mezzi di identificazione elettronica adatti al riconoscimento:

a) la tessera CNS (Carta nazionale dei Servizi);
b) la TS-CNS (Tessera Sanitaria – Carta Nazionale dei Servizi);
c) la CIE (Carta di Identità Elettronica)
d) la CRS (Carta Regionale dei Servizi)

e) Le identità digitali rilasciate nel contesto del sistema SPID di livello 2 o superiore.
f) Le identità digitali rilasciate nel contesto di identificazione elettronica riconosciuto da uno stato membro EU ex artt. 8 e 24 eIDAS.

Nei casi a,b,c,d di cui sopra il Richiedente, previo inserimento del PIN, effettua l'autenticazione sul portale del Certificatore o del CIE ID Server (caso CIE). Il sistema recupera le informazioni anagrafiche inserite nel Certificato digitale e le associa a quelle relative al Certificato di sottoscrizione in oggetto di richiesta.
Nel caso e, il Richiedente, utilizzando le credenziali SPID di livello 2 o superiore, è chiamato ad effettuare un'autenticazione presso il portale del Certificatore o di una sua LRA attraverso strumenti messi a disposizione dal circuito SPID.
L'accesso alla funzionalità di richiesta del Certificato avviene mediante autenticazione di livello 2 o superiore previa l'utilizzo di credenziali SPID rilasciate dal Gestore dell'Identità.
Qualora l'identità digitale utilizzata sia stata emessa da un Gestore diverso da Namirial, la richiesta e rilascio del Certificato avvengono in conformità all'Avviso n. 17 di AgID del 24 gennaio 2019 recante *"Utilizzo identità digitali SPID al fine di rilasciare Certificati Qualificati".* In particolare, il Certificato conterrà l'OID 1.3.76.16.5, registrato dall'Agenzia, con la seguente descrizione: "Certificate issued through Sistema Pubblico di Identità Digitale (SPID) digital identity, not usable to require other SPID digital identity".
I dati di registrazione sono conservati, in questi casi, esclusivamente in formato elettronico.

3.3.6 Identificazione mediante processi conformi alla Normativa PSD2

Istituti bancari e società di servizi ad essi collegate possono offrire ai propri clienti la possibilità di rilasciare una Firma Elettronica Qualificata contestualmente ed ai fini dell'utilizzo dei propri servizi. Un utente già in possesso di un conto corrente può agevolmente richiedere un certificato qualificato semplicemente fornendo le proprie credenziali bancarie in fase di identificazione.
Il riconoscimento dei Richiedenti avviene tramite LRA censite ed operanti per conto del Certificatore.
Il riconoscimento viene eseguito secondo una delle modalità individuate al punto 3.3 tramite processi esterni a Namirial che siano autorizzati AgID e conformi all'art. 24 eIDAS.
I processi in questione debbono soddisfare un livello di autenticazione che sia pari, almeno, al livello *significativo* in conformità con l'art.8 del Regolamento ed operare secondo le normative AML locali, nonché secondo la Direttiva (UE) 2015/2366 e s.m.i. del Parlamento europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno (PSD2).
Tale normativa prevede che il Richiedente, dopo aver fornito i propri documenti di riconoscimento, possa essere identificato anche tramite gli attributi collegati al proprio account bancario, trustati tramite autenticazione presso il proprio servizio di online banking.

A identificazione conclusa, il Certificatore in possesso del dataset necessario può emettere un Certificato di Firma Qualificata.

3.3.7 Soluzioni certificate da AgID

Sono già state certificate e riconosciute da AgID alcune soluzioni sia in conformità all'art. 24 eIDAS, che alla normativa tedesca Geldwäschegesetz (GwG).
Tra queste, si citano:

- Check24;
- Autoident by IDNow;
- NECT;
- SignID;
- WebID;
- UMB.

3.4 Certificati Qualificati per Persone Giuridiche

Nel processo di emissione di Certificati Qualificati a Persone Giuridiche, il Titolare coincide con la persona giuridica a cui sarà intestato il Certificato Qualificato di Sigillo, il Richiedente coincide con la persona fisica che sottopone la richiesta al Certificatore ed espleta la fase di identificazione. L'identificazione avviene "de visu" o mediante Certificato di firma Qualificato.
La procedura di identificazione e registrazione degli utenti si articola sostanzialmente nelle seguenti fasi:

- identificazione "de visu" o mediante Certificato di firma Qualificato;
- sottomissione della richiesta, corredata della necessaria documentazione;
- verifica delle informazioni fornite ed accettazione o rifiuto della richiesta.

Le modalità di identificazione de visu o mediante Certificato di firma Qualificato avvengono secondo quanto descritto rispettivamente ai paragrafi 3.3.1 e 3.3.4.

3.5 Identificazione ed Autenticazione per il rinnovo delle chiavi e dei Certificati

Il rinnovo dei Certificati deve rispettare le seguenti condizioni:

- i Certificati non devono essere scaduti,
- la richiesta di rinnovo deve essere presentata negli ultimi 90 giorni di validità.

I Certificati che soddisfano queste condizioni ed emessi su dispositivi fisici possono essere rinnovati solo una volta.
I soggetti, 90 giorni prima della data di scadenza, riceveranno una e-mail che ricorderà loro la scadenza e spiegherà le procedure da seguire. Nel caso in cui non venga effettuato il rinnovo, verranno inviati altri alert 30 e 10 giorni di preavviso prima della scadenza.

I soggetti accedono a una procedura online che identifica il Richiedente, e convalida la sua identità, attraverso l'esecuzione di firme digitali con il Certificato la cui durata è prossima alla scadenza (maggiori dettagli sono descritti nella relativa guida utente disponibile in https://support.namirial.com)
Se la richiesta viene avanzata dopo la scadenza del Certificato, verrà eseguita una nuova registrazione ed emissione.

3.6 Identificazione ed Autenticazione per la richiesta di sospensione e revoca

Richiedente, Titolari e Terze Parti possono richiedere la sospensione o la revoca del Certificato. Le procedure per tali richieste sono:

- **procedura on-line**: servizio di revoca on-line cui si accede tramite il seriale del dispositivo e un apposito codice di revoca. Questa opzione è disponibile solo per il Titolare perché è l'unico a conoscenza dei propri codici personali. La richiesta di revoca o sospensione del Certificato Qualificato viene presentata al Certificatore compilando in tutte le sue parti l'apposito modulo messo a disposizione sul sito (https://support.namirial.com);
- **procedura di richiesta fisica**: Questa opzione è disponibile per tutti gli utenti (Richiedente, Titolare e Terza Parte) e viene effettuata attraverso un modulo cartaceo di richiesta che l'utente deve scaricare dal sito web della CA e presentare compilato e firmato di conseguenza.

Per entrambe le modalità, la richiesta di revoca contiene la data a partire dalla quale il Certificato sarà revocato.
La richiesta di sospensione contiene la data di inizio.
La Certification Authority verifica l'autenticità della richiesta e procede alla revoca del Certificato inserendo lo stesso nella lista dei Certificati revocati e sospesi (CRL) che gestisce.

4. Requisiti operativi del ciclo di vita dei Certificati

Questa sezione descrive le modalità con le quali opera il Certificatore ed in particolare l'organizzazione e le funzioni del personale addetto al servizio di certificazione, le modalità di richiesta del Certificato e le modalità di comunicazione con il Richiedente il Certificato ovvero con il Titolare del Certificato.
Se non diversamente indicato nel presente documento e in accordo con lo standard ETSI 319-411, i seguenti requisiti operativi sono applicati al ciclo di vita del Certificato. Tutte le entità incluse nel dominio Namirial (RA, LRA, Richiedenti, Titolari o altri partecipanti) devono notificare a Namirial CA tutte le modifiche alle informazioni riportate su un Certificato durante il suo periodo di validità e fino alla sua scadenza o revoca. La CA Namirial emetterà, revocherà o sospenderà i Certificati solo in risposta a richieste autenticate ed approvate.

4.1 Soggetti che possono richiedere il rilascio di un Certificato

Il Certificatore rilascia certificati per

Persone fisiche:

- indipendenti (certificati personali);
- appartenenti ad Organizzazioni;
- appartenenti ad Ordini Professionali.

Persone giuridiche:

- Certificato rilasciato all'Organizzazione o all'Ordine (Sigillo Elettronico);

I Certificati rilasciati possono essere relativi a:

- chiavi di sottoscrizione generate per l'uso attraverso applicazioni di firma remota
- chiavi di sottoscrizione generate per l'uso attraverso applicazioni di firma remota "disposable" con limitata disponibilità temporale (si veda relativo addendum)
- chiavi di sottoscrizione generate per la firma attraverso dispositivi di firma fisici;
- chiavi di sottoscrizione generate per la firma attraverso applicazioni di sottoscrizione automatica;
- chiavi di sottoscrizione generate per l'applicazione di Sigillo Elettronico

In tutti i casi, i Richiedenti e i Titolari sono soggetti a un processo di registrazione, che richiede i seguenti requisiti:

- Compilazione di un apposito modulo;
- Accettazione delle Condizioni Generali

4.1.1 Richiesta del Certificato

Le condizioni per l'identificazione e autenticazione sono descritte nel dettaglio al Capitolo 3.

4.2 Registrazione degli utenti

Le procedure per la registrazione del Richiedente (e Titolare nel caso non coincida con il Richiedente) e il rilascio del Certificato prevedono:

- che il Richiedente ed il Titolare vengano identificati con certezza dal Certificatore con una delle modalità descritte ai precedenti paragrafi.
- che il Richiedente ed il Titolare abbiano preso visione dell'informativa di cui all'art. 13 del GDPR
- che il Richiedente e il Titolare abbiano espresso il consenso alla videoregistrazione ed al trattamento dei dati, nel caso di videoidentificazione;
- che il Richiedente e Titolare abbiano preso visione delle Condizioni Generali di contratto e del presente Manuale Operativo;
- che il Richiedente e Titolare sottoscrivano il Modulo di Richiesta di Emissione del Certificato Qualificato (reperibile dalla sezione "Documenti" del sito https://docs.namirialtsp.com), debitamente compilato in tutte le sue parti;

Se è richiesto l'inserimento del Ruolo e del Terzo Interessato nel Certificato Qualificato devono essere inoltre forniti:

- documento dell'Organizzazione su carta intestata, recante data e numero di protocollo, che autorizza all'inserimento dei dati nel Certificato Qualificato del Richiedente, non antecedente a 30 (trenta) giorni dalla data di richiesta di registrazione;
- attestazione che l'Organizzazione ha ricevuto l'informativa di cui all'art. 13 del GDPR.

Se è richiesto l'inserimento del Titolo e/o Abilitazione Professionale nel Certificato Qualificato deve essere inoltre fornito:

- documento rilasciato da Ordine/Albo/Collegio professionale che attesti l'effettiva appartenenza, non antecedente a 30 (trenta) giorni dalla data di richiesta di registrazione.

Esclusivamente nel caso in cui il Richiedente coincida con i dati contenuti nel campo Subject del Certificato, esso assume la qualifica di Titolare.

4.3 Processo di registrazione

I partecipanti al processo di registrazione (Titolari, Richidenti, LRA, RAO, IR) concorrono al buon esito dell'emissione del Certificato, ciascuno assolvendo alle proprie responsabilità.

Il Certificatore, terminata la fase di identificazione, effettua l'operazione di registrazione del Richiedente/Titolare attraverso il portale web del servizio di certificazione digitale, il quale registra i dati forniti all'interno del proprio database. Il Certificatore provvede successivamente al rilascio del Certificato Qualificato e, ove previsto, alla consegna del dispositivo di firma.
Le attività di registrazione, oltre che essere svolte direttamente dal personale autorizzato del Certificatore, possono essere svolte dal personale delle LRA, i RAO, o dal personale indicato come IR, dopo apposito corso di formazione.

4.4 Elaborazione della richiesta

Attributi persona fisica

I Certificati emessi alla persona fisica possono essere:

- Personale, in questo caso Richidente e Titolare coincidono
- Il Titolare appartiene ad un'Organizzazione
- Il Titolare appartiene ad un Ordine Professionale

Gli attributi acquisiti dalla CA funzionali all'emissione dei Certificati e riferiti al Titolare sono:

- Nome e cognome
- Data di nascita
- Luogo di Nascita

Codice Fiscale se il Titolare è cittadino italiano. Nel caso in cui il Titolare sia cittadino estero, vengono acquisiti i dati specificati nell'apposita sezione 3.1.3 Univocità dei nomi

- Estremi del documento di riconoscimento
- Indirizzo fisico di residenza ed indirizzo email
- Indirizzo PEC se corrispondente alla modalità individuata per la trasmissione della password necessaria all'apertura busta cieca
- Recapito mobile se corrispondente alla modalità individuata per la trasmissione della password necessaria all'apertura busta cieca

Attributi persona giuridica

I Certificati emessi alla persona giuridica consistono in Sigilli Elettronici (QES)

Gli attributi acquisiti dalla CA funzionali all'emissione dei Certificati sono:

- Codice fiscale
- Partita iva
- Ragione sociale
- Sede legale
- Indirizzo e-mail
- Indirizzo PEC
- Recapito mobile

4.5 Emissione del Certificato

Qualora l'esito delle verifiche degli attributi di cui ai precedenti paragrafi sia positivo, viene inviata alla CA la richiesta di emissione del Certificato per la persona fisica o giuridica.
In caso contrario, la Certification Authority può rifiutarsi di portare a termine l'emissione del Certificato, ad esempio se le informazioni sono assenti, incomplete o inconsistenti, se sussistono dubbi sull'identità del Titolare o del Richiedente o se la documentazione fornita non è conforme a quanto disposto dal Certificatore.

4.6 Procedura di generazione delle chiavi

La procedura di generazione delle chiavi prevede i seguenti step:

- assegnazione al Titolare di un codice identificativo univoco nell'ambito degli utenti del Certificatore (CUC), diverso per ogni Certificato emesso;
- generazione del Certificato contenente la chiave pubblica e i dati previsti mediante la firma con la chiave di certificazione della CA;
- inserimento del Certificato nel registro dei Certificati;
- registrazione sul giornale di controllo dell'avvenuta generazione;
- trasmissione del Certificato dalla CA alla LRA;
- inserimento del Certificato nel dispositivo di firma;
- verifica dell'inserimento del Certificato nel dispositivo di firma;
- cancellazione dal DB del record cifrato della busta cieca associata al Titolare: questa avviene non appena viene ricevuto l'SMS o la PEC per l'apertura;
- registrazione sul giornale di controllo dell'avvenuta personalizzazione del dispositivo di firma.

4.7 Accettazione del Certificato

Il Certificatore non prevede alcun comportamento concludente al momento del rilascio del Certificato. Quest'ultimo si intende accettato alla sua emissione.

4.8 Coppia di chiavi e utilizzo del Certificato

Il proprietario del Certificato deve salvaguardare la propria chiave privata, facendo attenzione ad evitarne la divulgazione a terzi. Namirial fornirà un apposito contratto di sottoscrizione, che evidenzia gli obblighi del proprietario in merito alla protezione della chiave privata. Le chiavi private devono essere utilizzate solo come specificato nei campi "keyUsage" ed "extendedkeyUsage", come riportato all'interno del relativo Certificato. Le responsabilità relative all'uso delle chiavi e dei Certificati includono quelle affrontate di seguito. al paragrafo 9.8.3. I Certificati devono essere usati solo come prescritto dalla Certificate Policy e dalle Condizioni Generali Qualsiasi uso diverso è proibito.

4.9 Modalità di consegna dei dispositivi di firma personali e dei codici segreti

I dispositivi fisici di firma, se presenti, vengono consegnati al Titolare dal RAO o dall'IR, successivamente all'identificazione e registrazione dello stesso
I seguenti codici di utilizzo sono relativi al Certificato e all'eventuale dispositivo fisico di firma:

- PIN del dispositivo virtuale (Certificato di firma remota, firma remota "disposable", firma automatica)
- PIN e PUK del dispositivo fisico (smarcard/token usb)
- Password del Sigillo elettronico

Tali codici vengono consegnati al Titolare successivamente all'emissione del Certificato in modalità sicura.

4.9.1 Modifica dei codici del Titolare

In qualsiasi momento successivo alla generazione del Certificato, il Titolare potrà modificare il *CodicePIN*.

4.9.1.1 Modifica PIN

Se il certificato risiede su dispositivo fisico il PIN può essere modificato dal Titolare sia all'interno del portale dei servizi del Certificatore, accedendo alla propria area riservata che tramite il software standalone messo a disposizione dal Certificatore.

4.10 Limitazioni d'uso

Ferma restando la responsabilità del Certificatore di cui al Dlgs. 82/2005 (Codice dell'Amministrazione Digitale, art.30 comma 1 lettera a), è responsabilità del Titolare verificare il rispetto dei limiti d'uso inseriti nel Certificato.
La richiesta di inserire altre specifiche limitazioni d'uso, il cui testo non potrà comunque superare 200 caratteri, sarà valutata dal Certificatore per gli aspetti legali, tecnici e di interoperabilità e valorizzata di conseguenza.
In considerazione dei limiti suddetti, il Certificatore adotta i limiti d'uso indicati dagli utenti, ai sensi dell'articolo 12, comma 6, lettera c) della Deliberazione CNIPA 45/2009 e successive modificazioni, e provvede ad inserire, su richiesta del Titolare o della persona giuridica che ha richiesto il Certificato, almeno i seguenti limiti d'uso:

- I Titolari fanno uso del Certificato solo per le finalità di lavoro per le quali esso è rilasciato. / *The certificate holder must use the certificate only for the purposes for which it is issued.*

- Il presente Certificato è valido solo per firme apposte con procedura automatica. / *This certificate may only be used for unattended/automated digital signatures.*
- L'utilizzo del Certificato è limitato ai rapporti con (indicare il soggetto). / *The certificate may be used only for relations with the (declare the subject).*

4.11 Rinnovo del Certificato

Il rinnovo deve essere effettuato, necessariamente, prima della scadenza del Certificato. La procedura può essere utilizzata per il rinnovo di un precedente Certificato emesso dalla Certification Authority nei casi in cui il Richiedente abbia un Certificato Qualificato valido e il corrispondente SSCD/QSCD fornito dalla stessa. La CA fornisce un'applicazione software che può generare la coppia di chiavi all'interno del Q/SSCD e la richiesta di Certificato PKCS # 10.

La procedura di riemissione delle chiavi richiede almeno i seguenti passi:

- Aggiornamento di alcuni dati del Titolare (es. Titolo, Organizzazione, ecc.) se vi è una richiesta da parte di un'entità a cui il Titolare è associato. In questo scenario, l'entità fornirà nuove informazioni;
- Assicurarsi che il Richiedente abbia il controllo esclusivo del Q/SSCD tramite l'esecuzione della firma con il Certificato precedente;
- Generazione di una nuova coppia di chiavi nel Q/SSCD e rilascio di un nuovo Certificato;
- Registrazione degli eventi rilevanti per l'iscrizione all'interno del giornale di controllo della CA

4.12 Modifica del Certificato

Un Certificato firmato dalla CA emittente non può essere modificato. Al fine di rimediare a potenziali imprecisioni subite durante il processo di generazione, è necessario emettere un nuovo Certificato e, per motivi di sicurezza, revocare il precedente. Nel caso in cui il Certificato emesso riporti informazioni errate, a causa di errori commessi dalla CA o dalla RA, il Certificato errato verrà revocato e ne verrà prontamente emesso uno nuovo senza alcun costo aggiuntivo per il cliente e senza richiedere ulteriori informazioni allo stesso. D'altra parte, se il Certificato emesso riporta informazioni errate a causa di errori commessi dal Richiedente (ad esempio la compilazione errata di uno o più campi del modulo di richiesta), il Certificato errato verrà revocato.

4.13 Revoca e sospensione del Certificato Qualificato

La sospensione o revoca del Certificato avviene nel rispetto degli articoli da 22 a 29 del DPCM 22 febbraio 2013, determina la fine della validità prima della scadenza naturale e invalida eventuali firme apposte successivamente al momento della pubblicazione della

lista di revoca che contiene il riferimento a tale Certificato. La pubblicazione della lista è attestata mediante adeguato riferimento temporale apposto dal Certificatore.
Le liste di revoca e sospensione (CRL) sono pubblicate nel registro dei Certificati con periodicità stabilita dall'art. 18, comma 4, della Deliberazione CNIPA n.45 del 21 maggio 2009 e successive modificazioni.
Il Certificatore può anticipare l'emissione della CRL in circostanze particolari.
La data della pubblicazione della lista, asseverata da un riferimento temporale, è riportata nel Giornale di Controllo del Certificatore, dove sono annotate sospensioni, revoche e riattivazione dei Certificati.
La sospensione del Certificato comporta la non validità delle firme generate durante il periodo di sospensione. Nel caso in cui si proceda alla revoca di un Certificato in stato di sospensione, la revoca decorre dalla data di inizio della sospensione.

4.13.1 Motivi per la revoca o sospensione del Certificato

Il mantenimento del Certificato Qualificato è sempre a cura del Certificatore, che deve:

- revocarlo in caso di cessazione dell'attività del Certificatore, fatto salvo indicare un Certificatore sostitutivo ai sensi dell'art. 37, comma 2 del Dlgs. 82/2005 (Codice dell'Amministrazione Digitale);
- revocarlo o sospenderlo in esecuzione di un provvedimento dell'autorità;
- revocarlo o sospenderlo a seguito di richiesta del Titolare o del Terzo Interessato dal quale derivino i poteri del Titolare, nei casi in cui:
- sia stato smarrito il dispositivo fisico,
- sia venuta meno la segretezza della chiave privata o delle credenziali di accesso al dispositivo di generazione della firma,
- si sia danneggiato il dispositivo fisico,
- si sia verificato un qualunque evento che abbia compromesso l'affidabilità della chiave,
- siano mutati i dati di riferimento del Titolare indicati nel Certificato, ivi compresi quelli relativi al Ruolo,
- si siano accertati abusi o falsificazioni,
- sia terminato il rapporto tra Titolare e Certificatore.

La sospensione può avvenire in seguito alle seguenti circostanze:

- richiesta di revoca di cui non è possibile accertare in tempo utile l'autenticità;
- interruzione della validità del Certificato per inutilizzo temporaneo.

Il Titolare ha facoltà di richiedere la revoca o sospensione del Certificato per un qualunque motivo dallo stesso ritenuto valido ed in qualsiasi momento.
La richiesta di revoca o sospensione del Certificato Qualificato viene inoltrata per iscritto al Certificatore, compilando in tutte le sue parti l'apposito modulo messo a disposizione sul sito della CA.

La richiesta di revoca contiene la data a decorrere dalla quale il Certificato sarà revocato. L'autenticità di tale richiesta viene verificata dal Certificatore che esegue la revoca inserendo il Certificato nella lista dei Certificati revocati e sospesi (CRL) da lui gestita.

4.13.2 Sospensione in emergenza

Il Titolare, in caso di smarrimento/compromissione della chiave privata o dei codici che ne consentono l'utilizzo, richiede tempestivamente al Certificatore la sospensione del Certificato.
La richiesta può essere inoltrata:

- telefonicamente[3] al servizio di Help Desk;
- via Web[4] inserendo il codice di emergenza o OTP.

Il Certificatore procede tempestivamente ad inserire il Certificato Qualificato nella lista dei Certificati revocati e sospesi (CRL).
Successivamente il Titolare/Terzo Interessato richiede per iscritto, al Certificatore, la revoca o la sospensione o la riattivazione del Certificato, motivandola.
L'eventuale revoca decorre dalla data di inizio della sospensione.

4.13.3 Modalità per l'inoltro delle richieste

La revoca, la sospensione o la riattivazione del Certificato può essere richiesta con le seguenti modalità:

- **Sito Web**, il Titolare/Terzo Interessato si collega al sito web del Certificatore, compilando l'apposito modulo elettronico. Per garantire l'autenticità della richiesta il Titolare prima di accedere al sistema deve autenticarsi ai servizi del Certificatore con le proprie credenziali e il codice OTP.
- **Cartacea**, il Titolare/Terzo Interessato scarica dal sito del Certificatore l'apposito modulo, compila il modulo in tutte le sue parti, si reca presso il Certificatore con un documento di riconoscimento in corso di validità o inoltra il modulo via fax con copia di un documento di riconoscimento in corso di validità.

Il Certificatore verifica l'autenticità della richiesta con le seguenti modalità:
se Titolare:

- verifica che la richiesta sia compilata in tutte le sue parti,
- verifica che il documento di riconoscimento sia in corso di validità;

se Terzo Interessato

- verifica che la richiesta sia compilata in tutte le sue parti,
- verifica l'esistenza del timbro o altra segnatura equivalente,
- verifica che il Richiedente sia il "Referente" indicato nella Convenzione,
- verifica che il documento di riconoscimento sia in corso di validità.

[3] Al cliente verranno richiesti alcuni dati personali per assicurare la liceità della richiesta.
[4] Il sito web è accessibile in modalità 24h x 7gg.

4.13.4 Tempi per la gestione delle richieste

Le richieste di revoca, sospensione e riattivazione dei Certificati Qualificati, saranno gestiti entro un giorno lavorativo dal ricevimento della richiesta, fermo restando che il Certificatore provvederà tempestivamente alla pubblicazione della nuova lista (CRL) in caso di richiesta di sospensione in emergenza.
Il momento della pubblicazione è asseverato da un riferimento temporale ed annotato nel giornale di controllo.

4.13.5 Comunicazione dell'avvenuta revoca o sospensione

Il Certificatore, dopo aver verificato l'autenticità della richiesta, provvede ad avvisare tempestivamente il Titolare e/o il Terzo Interessato con le seguenti modalità:

- se la richiesta è su iniziativa del Titolare, il Certificatore verifica se nel Certificato sono presenti informazioni relative all'Organizzazione. In tal caso provvede a comunicare via e-mail, al Terzo Interessato, l'avvenuta revoca o sospensione;
- se la richiesta è su iniziativa del Terzo Interessato, il Certificatore comunica via e-mail, al Titolare e al Terzo Interessato, l'avvenuta revoca o sospensione del suo Certificato;
- se la richiesta è su iniziativa del Certificatore, il Certificatore comunica via e-mail, al Titolare, l'intenzione di revocare o sospendere il Certificato, indicando la motivazione nonché la data e l'ora di decorrenza; se nel Certificato è presente l'Organizzazione, comunica via e-mail al Terzo Interessato se aveva sottoscritto la Convenzione, la variazione di stato del Certificato.

4.14 Servizio di verifica dello stato del Certificato

La CA Namirial fornisce servizi di controllo per verificare lo stato del Certificato, come CRL e OCSP. Lo stato del Certificato (che potrebbe essere attivo, sospeso o revocato) è reso disponibile a tutte le entità coinvolte pubblicando la Certificate Revocation List (CRL). La CA rende anche disponibile un OCSP (On-line Certificate Status Provider) al seguente link: http://ocsp.namiriatsp.com/ocsp/certstatus. La CRL è firmata al momento della sua emissione, con il Certificato della CA.
Sia la CRL che l'OCSP sono disponibili 24 ore per 7 giorni la settimana.

4.15 Modalità di sostituzione delle chiavi

4.15.1 Sostituzione delle chiavi di sottoscrizione degli utenti

La durata massima di un Certificato Qualificato è di 6 (sei) anni. La richiesta di rinnovo delle chiavi deve essere effettuata prima della scadenza del Certificato (dal 45° giorno prima della data di scadenza).

Il rinnovo del Certificato può essere fatto solo dal Certificatore Qualificato che l'ha emesso ed il Titolare può procedere a tale operazione mediante la procedura remota disponibile nel software messo a disposizione dal Certificatore.

La procedura di rinnovo prevede:

- l'eventuale aggiornamento dei dati relativi al Titolare con le informazioni fornite dal Terzo Interessato (se presente);
- la verifica del possesso del dispositivo di firma contenente il Certificato in scadenza, mediante procedura remota;
- la generazione di una nuova coppia di chiavi sul dispositivo sicuro di firma ed emissione di un nuovo Certificato, mediante procedura remota;
- la registrazione sul Giornale di Controllo dell'avvenuta operazione.

Se nel Certificato Qualificato sono presenti anche informazioni relative al Ruolo e all'Organizzazione, il Certificatore provvederà ad inserirle nel nuovo Certificato verificando, al momento del rinnovo, che non sia pervenuta la revoca del Certificato da parte del Terzo Interessato.
Qualora le informazioni relative al Ruolo e all'Organizzazione contenute nel Certificato da rinnovare non siano più valide al momento del rinnovo, al Titolare che intenda effettuare il rinnovo attraverso la procedura remota verrà rilasciato un Certificato privo di tali informazioni.
Nel caso di richiesta effettuata dopo la scadenza del Certificato si procederà ad una nuova registrazione ed emissione.
Qualora si rendesse necessaria la sostituzione del Certificato Qualificato, a causa di variazioni delle informazioni in esso contenute, si procederà con la revoca di tale Certificato e/o con una nuova emissione.

4.15.2 Sostituzione delle chiavi di Marcatura Temporale

Le chiavi di Marcatura Temporale sono sostituite dopo non più di 3 (tre) mesi di utilizzo, indipendentemente dalla durata del loro periodo di validità e senza revocare il corrispondente Certificato, in conformità all'art. 49, comma 2 del DPCM 22 febbraio 2013.
I Certificati relativi alle chiavi di Marcatura Temporale hanno durata massima pari a 11 (undici) anni.

4.15.3 Sostituzione delle chiavi di certificazione

Avviene nel rispetto dell'art. 30 del DPCM 22 febbraio 2013. Il Certificato "Root" della CA utilizzato dal Certificatore per sottoscrivere i Certificati Qualificati del Titolare ha durata 20 anni e viene sostituito all'occorrenza per garantire la fruibilità di tutti i Certificati emessi fino alla naturale scadenza degli stessi.

4.16 Risoluzione della sottoscrizione

Il contratto di servizio, sottoscritto dalla CA e dal cliente, si considera terminato alle seguenti date:

- data di scadenza del Certificato;
- data di revoca del Certificato.

4.17 Key escrow e recupero delle chiavi

L'escrow delle chiavi non è permesso per le chiavi CA. Le chiavi private della CA non vengono custodite, ma sono cifrate all'interno di file utilizzabili esclusivamente all'interno dello specifico HSM e all'interno del proprio Security World.
L'utilizzo delle chiavi all'interno degli HSM è consentito soltanto con un quorum di carte OCS adeguato (2/6), mentre per l'impostazione del Security World il quorum è soddisfatto con l'utilizzo di 3/6 carte.

5. Controlli e misure di sicurezza

Il sito primario di produzione (Data4) è localizzato a Milano, mentre il sito di Disaster Recovery è collocato a Senigallia all'interno degli edifici Namirial.
Sono definite politiche, responsabilità e procedure operative per l'accesso alle aree protette di Data4. In queste aree sono implementati dispositivi di protezione fisica per minimizzare i rischi legati ad accessi non autorizzati. La protezione è implementata da sistemi di controllo degli accessi e da sistemi di videosorveglianza posizionati nei punti più critici e segnalati da apposita cartellonistica. Il sito di Disaster Recovery è collocato all'interno degli edifici Namirial e rispondente ai criteri di sicurezza conformi a quanto richiesto da normativa.

5.1 Controlli fisici

Le aree di lavoro sono sottoposte a diverse misure di controllo, in relazione ai rischi, al valore degli asset e alle informazioni da proteggere. Un processo di autorizzazione organizzato, relativo al tipo di area, gestisce tutti gli accessi.

5.1.1 Collocazione del sito

Namirial esegue le sue operazioni CA da data center sicuri e dotati di controlli logici e fisici che rendono le operazioni CA Namirial inaccessibili a personale non autorizzato.
Il data center primario è collocato presso il Campus di Data4 (Cornaredo, MI), mentre il sito di Senigallia funge da Disaster Recovery. Namirial opera in conformità ad una politica di sicurezza progettata per rilevare, scoraggiare e prevenire l'accesso non autorizzato alle operazioni dell'Organizzazione.

5.1.2 Accessi fisici

Le attrezzature Namirial sono protette da accessi non autorizzati su cui sono implementati controlli fisici per ridurre il rischio di manomissione delle attrezzature. Le parti sicure delle strutture di hosting sono protette mediante controlli di accesso fisici che le rendono accessibili solo a persone debitamente autorizzate. Gli edifici sono sotto costante sorveglianza video.
L'accesso alla sala del Datacenter è regolamentato dalle procedure Data4. All'esterno del Data Center sono affisse le norme di accesso e di comportamento da tenere all'interno del Data Center.

5.1.3 Energia elettrica e condizionamento

I Data Center hanno alimentatori primari e secondari che assicurano un accesso continuo e ininterrotto all'energia elettrica. Gli alimentatori ininterrotti (UPS) e i generatori elettrici

forniscono un'alimentazione di backup ridondante. Le strutture dei Data Center utilizzano sistemi multipli per il riscaldamento, il raffreddamento e la ventilazione dell'aria.

5.1.4 Esposizione all'acqua

Un sistema di rilevamento rileva la presenza di liquido attraverso dei sensori e determina lo scatto dell'allarme in caso di allagamento.

5.1.5 Prevenzione degli incendi

I Data Center sono dotati di meccanismi di soppressione degli incendi.

5.1.6 Media storage

Gli asset dai danni accidentali e dall'accesso fisico non autorizzato.

5.2 Controlli procedurali

5.2.1 Trusted roles

Il personale nominato secondo i trusted roles previsti dallo standard ETSI EN 319-401 include gli operatori addetti all'amministrazione del sistema CA e RA. Le funzioni e i compiti svolti dai trusted roles sono distribuiti per permettere che una sola persona autonomamente non possa aggirare le misure di sicurezza o sovvertire la sicurezza e l'affidabilità delle operazioni della PKI. Tutto il personale nominato secondo trusted roles deve essere libero da conflitti di interesse che possano essere pregiudizievoli a livello di imparzialità nelle operazioni della PKI Namirial.
I trusted roles sono nominati dal management. Un elenco del personale nominato in tali ruoli viene mantenuto e rivisto dall'Organizzazione. Le responsabilità previste dai trusted roles sono le seguenti:

- Responsabili della sicurezza (Security Officers): Responsabilità della definizione delle policy di sicurezza.
- Amministratori di sistema: Autorizzati a installare, configurare e mantenere i sistemi trust Namirial per la gestione del servizio
- Operatori di sistema: Responsabili del funzionamento quotidiano dei sistemi trust Namirial. Sono autorizzati ad eseguire il backup del sistema.
- Auditor di sistema: Autorizzati a visualizzare gli archivi e i log di audit dei sistemi trust Namirial.

5.2.2 Numero delle persone coinvolte nelle attività

In caso di compiti relativi a funzioni critiche, Namirial richiede che almeno due persone agiscano in un trusted role per evitare che una persona possa agire in autonomia.

Quando questo meccanismo è attivo, due persone autorizzate sono tenute ad applicarlo ove opportuno.

5.2.3 Identificazione ed autenticazione per ciascun ruolo

Il personale preposto a questi servizi è tenuto ad autenticarsi ai sistemi CA e RA prima di accedere agli ambienti necessari per svolgere i propri ruoli di fiducia.

5.2.4 Attività che richiedono il dual control

Le attività che richiedono la segregation of duties sono le seguenti:

- La verifica delle informazioni nella generazione di Certificati CA (root e intermedi, ove applicabile);
- L'approvazione delle richieste di Certificati CA;
- La maggior parte dei compiti relativi alla gestione delle chiavi CA o all'amministrazione CA.

Namirial, per queste attività individua tra i propri dipendenti delle figure adeguate ai trusted roles definiti in precedenza, cui può essere assegnato solo un ruolo tra amministratore o auditor, ma entrambi possono ricoprire anche il ruolo di operatore.

5.3 Controlli sul personale

Queste figure possiedono adeguata esperienza nella definizione, sviluppo e gestione di servizi PKI ed hanno ricevuto un necessario livello di formazione su procedure e strumenti che possono essere utilizzati in varie fasi operative.
Il personale Namirial incaricato a queste attività deve:

- possedere la competenza, l'affidabilità, l'esperienza e le qualifiche necessarie e aver ricevuto formazione relativa alle norme di sicurezza e di protezione dei dati personali adeguata ai servizi offerti e alla loro funzione lavorativa;
- essere in grado di soddisfare il requisito di "conoscenza, esperienza e qualifiche" attraverso formazione o esperienza effettiva, o una combinazione di entrambe;
- essere aggiornato circa le nuove minacce e sulle più recenti pratiche di sicurezza applicabili.

5.3.1 Qualifiche, esperienza e requisiti di autorizzazione

Namirial assume personale con i più alti livelli di integrità e competenza. Non esiste alcun requisito di cittadinanza per il personale che svolge i trusted roles associati all'emissione di altri tipi di Certificati.

5.3.2 Check delle esperienze pregresse

Namirial verifica l'identità ed esegue un controllo delle esperienze pregresse di ogni dipendente al fine di affidare uno dei trusted roles previsti ed indicati in precedenza.

5.3.3 Requisiti di formazione

Tutto il nuovo personale Namirial riceve una formazione di base sulla security awareness durante il processo di onboarding a livello aziendale. Oltre a ciò, una formazione on-the-job dedicata viene fornita a tutto il personale Namirial coinvolto in compiti specifici, come descritto nel presente documento.

5.3.4 Frequenza di aggiornamento della formazione e requisiti

Il personale è tenuto a mantenere alti livelli di competenza attraverso sessioni di formazione pertinenti al settore per poter continuare ad agire in conformità ai requisiti richiesti dai trusted roles. Namirial mette al corrente di eventuali modifiche circa la normale operatività tutti coloro che ricoprono tali ruoli.

5.3.5 Frequenza della job rotation

In caso di job rotation, Namirial esegue un controllo di sicurezza, compresa una verifica delle credenziali a livello di reti, sistemi, applicazioni o altre risorse utilizzate, nonché le autorizzazioni di accesso alle strutture e alle aree.

5.3.6 Sanzioni in caso di azioni non autorizzate

Il personale Namirial che non segue le politiche e le disposizioni interne all'Organizzazione, sia per negligenza che per dolo, è soggetto ad sanzioni amministrative o disciplinari, compresa la cessazione del rapporto di lavoro o di collaborazione e, nei casi più gravi a sanzioni penali.

5.3.7 Requisiti del personale non dipendente

Il personale non dipendente, che sia stato incaricato di un trusted role, è soggetto ai requisiti ed ai doveri specifici di tale ruolo nonché alle eventuali sanzioni.

5.3.8 Documentazione fornita al personale

Al personale, in fase di onboarding, viene fornita le informazioni necessarie per svolgere i propri compiti, compresa una copia del presente documento e la documentazione operativa necessaria per mantenere l'integrità delle operazioni della CA Namirial.

5.4 Procedure di gestione del giornale di controllo

Namirial registra tutte le informazioni rilevanti relative ai dati emessi e ricevuti dalla stessa e mantiene le registrazioni accessibili per un periodo di 20 anni, allo scopo di fornire prove adeguate in procedimenti legali e garantire la continuità del servizio.

5.4.1 Frequenza di salvataggio del giornale di controllo

La frequenza di salvataggio del giornale di controllo è giornaliera.
L'ora esatta di significativi eventi ambientali, di gestione delle chiavi e di sincronizzazione dell'orologio di Namirial sono registrati. L'ora utilizzata per registrare gli eventi come richiesto nel giornale di controllo deve essere sincronizzata con UTC almeno una volta al giorno.

5.4.2 Conservazione delle registrazioni del giornale di controllo

La procedura messa in atto dal Certificatore prevede che gli eventi rilevati e disponibili sul database vengano estratti ed inseriti all'interno di file di testo gestiti in maniera tale da garantirne l'integrità e la disponibilità.
Le registrazioni relative al funzionamento dei servizi sono a disposizione dell'Autorità Giudiziaria nel caso di procedimenti legali ed internamente ai fini di audit e verifiche periodiche del sistema.

5.4.3 Backup del giornale di controllo

La sincronizzazione degli eventi con il repository presente sul sito di Disaster Recovery avviene con frequenza almeno giornaliera.

5.5 Archiviazione dei record

Namirial produce e conserva registri accessibili che comprendono tutte le attività e tutte le informazioni rilevanti relative ai dati emessi e ricevuti da Namirial.
La CA mantiene i registri accessibili per un periodo di 20 anni, allo scopo di fornire prove adeguate in procedimenti legali e garantire la continuità del servizio. Questi registri restano accessibili anche nel caso in cui Namirial abbia cessato le proprie attività.
Le principali evidenze raccolte sono:

- Richieste di emissione;
- Documentazione fornita dai Richiedenti;
- CSR (Certificate Signing Request) fornite dai Richiedenti;
- Dati personali del Richiedente e del Titolare (se sono entità diverse);
- Richieste di revoca o sospensione;
- Tutti i Certificati emessi;
- Giornale di controllo per 20 anni.

5.6 Sostituzione della chiave

Nel caso in cui l'utente finale (Titolare) decida di utilizzare una nuova chiave, deve necessariamente richiedere un nuovo Certificato.

5.7 Compromissione della chiave e disaster recovery

La compromissione della chiave di certificazione rappresenta un evento critico, che innescherebbe l'attivazione del Piano di Cessazione condiviso con AgID, che consiste nelle attività descritte all'interno dell'omonimo paragrafo.
La continuità operativa è garantita anche in situazioni di elevata criticità o disastro.

5.8 Piano di cessazione

Namirial ha definito un piano di cessazione aggiornato. In particolare, secondo tale procedura interna, Namirial dovrà:

- informare almeno 60 giorni prima della cessazione i seguenti soggetti: tutti i Richiedenti e gli altri soggetti con i quali Narmirial ha accordi o relazioni, tra cui i Destinatari e le autorità competenti (AgID e l'organismo di certificazione). Inoltre, queste informazioni devono essere messe a disposizione di altre parti facenti affidamento;
- porre fine all'autorizzazione di tutti i subappaltatori ad agire per conto di Namirial nello svolgimento di qualsiasi funzione relativa al processo di emissione di Certificati;
- trasferire gli obblighi a una parte affidabile per il mantenimento di tutte le informazioni necessarie a fornire la prova del funzionamento di Namirial per un periodo ragionevole, a meno che non sia possibile dimostrare che Namirial non detenga alcuna informazione;
- le chiavi private devono essere distrutte, o ritirate, per assicurare che non possano essere recuperate;
- prendere accordi per trasferire la fornitura di servizi fiduciari per i suoi clienti esistenti ad un altro Trust Service Provider.

La Certification Authority ha redatto il proprio "Piano di Cessazione" ad uso esclusivo del Certificatore ed in conformità all'art. 24 eIDAS.

6. Controlli di sicurezza tecnica

6.1 Generazione della coppia di chiavi

La CA emette il Certificato Qualificato in conformità con il regolamento (UE) n. 910/2014.
Le chiavi di certificazione utilizzate per la firma dei Certificati sono generate per mezzo di dispositivi e procedure che garantiscono l'unicità, la segretezza e la resilienza della chiave privata.
La CA utilizza una coppia di chiavi crittografiche di almeno 4096 bit generate all'interno di HSM (Hardware Secure Module).

Gli HSM e le procedure assicurano che:

- le coppie di chiavi siano generate individualmente, sempre in copia unica;
- le coppie di chiavi soddisfino i requisiti imposti dagli algoritmi di generazione e dalle verifiche RSA perché gli HSM possiedono un motore interno di generazione di coppie di chiavi RSA e DSA;
- la generazione di tutte le coppie di chiavi possibili è equiprobabile;
- la persona che attiva le procedure di generazione è sempre identificata;
- la generazione delle coppie di chiavi avviene esclusivamente all'interno dell'HSM;
- se i dispositivi sono preparati o gestiti da una terza parte, Namirial verifica che questa terza parte abbia i requisiti adeguati.

Nelle attività di certificazione, Namirial utilizza l'algoritmo RSA.
La generazione di coppie di chiavi di certificazione da parte della CA è sotto doppio controllo, secondo la procedura della Key Ceremony.

6.2 Modalità di generazione delle chiavi

La generazione della coppia di chiavi asimmetriche (pubblica e privata) è effettuata mediante dispositivi e procedure che assicurano, in rapporto allo stato delle conoscenze scientifiche e tecnologiche, l'unicità e la robustezza delle chiavi generate, nonché la segretezza della chiave privata. Il sistema di generazione delle chiavi assicura:

- la rispondenza della coppia ai requisiti imposti dagli algoritmi di generazione e di verifica utilizzati;
- l'equiprobabilità di generazione di tutte le coppie possibili;
- l'identificazione del soggetto che attiva la procedura di generazione.

Le chiavi appartenenti ad una delle tipologie elencate nell'art. 5, comma 4, del DPCM 22 febbraio 2013 sono generate (art. 6 e 7), conservate (art. 8) ed utilizzate (art. 11, comma 1) all'interno di uno stesso dispositivo elettronico avente le caratteristiche di sicurezza di cui all'art. 12 del DPCM di cui in precedenza.
La generazione delle chiavi avviene all'interno del dispositivo sicuro per la generazione delle firme.

Nel caso in cui la generazione avvenga al di fuori di tale dispositivo, il sistema di generazione è conforme alle disposizioni di cui all'art. 9 del DPCM 22 febbraio 2013.
Nel caso di Certificato abbinato ad una CNS, la generazione delle chiavi di firma può avvenire centralmente ed anche al di fuori della CNS stessa; inoltre, essa può essere svolta presso il Certificatore secondo gli specifici accordi in essere con la PA emittente, comunque nel rispetto dello standard RFC 3161 (X.509 Public Key Infrastructure Time Stamp Protocol) e dell'art. 9 del DPCM 22 febbraio 2013.
Le chiavi corrispondenti a Certificati Qualificati per Sigillo Elettronico sono generate utilizzando le stesse procedure adottate per la generazione delle chiavi corrispondenti a Certificati Qualificati per Firma Elettronica.

6.2 Modalità di generazione delle chiavi di certificazione

La generazione delle chiavi asimmetriche avviene all'interno dei moduli crittografici dedicati e certificati in presenza del Responsabile del servizio di Certificazione, come previsto dall'art. 7 del DPCM 22 febbraio 2013 ed è generata solo con la presenza contemporanea di due operatori incaricati all'uopo.

6.2.1 Modalità di generazione delle chiavi di sottoscrizione degli utenti

Completata la fase di registrazione, durante la quale i dati del Richiedente e del Titolare vengono memorizzati nel database del Certificatore, è possibile procedere alla generazione delle chiavi di sottoscrizione. Questa operazione può avvenire in due diverse modalità:

- Chiavi generate dal Certificatore (o LRA).
- Chiavi generate dal Richiedente.

In ogni caso, avendo a disposizione il dispositivo di firma, il Titolare o gli operatori RA/RAO, potranno generare una nuova coppia di chiavi mediante la funzione di generazione di chiavi asimmetriche dello stesso dispositivo.
I dispositivi di firma utilizzati rispondono ai requisiti di sicurezza previsti dalla normativa.
Le chiavi corrispondenti a Certificati Qualificati di Sigillo Elettronico possono essere generate solo dal Certificatore.

6.2.1.1 Chiavi generate dal Certificatore

Questa procedura viene effettuata dagli operatori RA del Certificatore presso i propri locali, o dagli operatori RAO delle LRA.
Sono effettuate le seguenti operazioni:

- l'operatore si autentica ai servizi del Certificatore, seleziona i dati di registrazione del Richiedente e attiva la procedura di richiesta di Certificato;
- l'applicazione accede al dispositivo di firma con il PIN di default e genera la coppia di chiavi.

6.2.1.2 Chiavi generate dal Richiedente

Rilascio self-enroll

Questa procedura prevede che la personalizzazione del dispositivo di firma sia svolta sotto il controllo dell'utente, o comunque in sua presenza, e si basa su interazioni telematiche sicure con il Certificatore (generalmente connessioni via Internet protette da protocolli che garantiscano un adeguato livello di sicurezza).
In questa fase le chiavi di sottoscrizione sono generate dal Richiedente stesso attivando con l'applicazione approvata dalla CA il dispositivo sicuro per la generazione della firma fornito o indicato dallo stesso Certificatore.

Il Richiedente è:

- riconosciuto dal Certificatore tramite un codice personale riservato o una password;
- autenticato dal dispositivo sicuro per la generazione della firma tramite l'inserimento del PIN contenuto nella busta cieca (scratch-card) consegnata a seguito dell'identificazione da parte dell'IR/RAO

Rinnovo

Questa procedura può essere utilizzata per le operazioni di rinnovo di un precedente Certificato generato dal Certificatore nei casi in cui il Richiedente disponga di un Certificato di sottoscrizione valido e del relativo dispositivo di firma fornito dal Certificatore. Il Certificatore fornisce allo scopo l'applicazione in grado di generare la coppia di chiavi all'interno del dispositivo di firma e la richiesta di Certificato in formato PKCS#10.
I prerequisiti hardware e software, nonché tutte le indicazioni per l'installazione del prodotto "FirmaCerta", sono riportate nella "Guida rapida all'utilizzo" del software, disponibile all'URL:

https://support.namirial.com/

Nel documento, che è parte integrante del presente Manuale Operativo, sono riportate le modalità operative per il rinnovo dei Certificati di firma.
Non ricadono in questa casistica le chiavi corrispondenti a Certificati Qualificati per Sigillo Elettronico.

6.2.3 Modalità di generazione delle chiavi di Marcatura Temporale

La generazione delle chiavi avviene nel rispetto degli art. 49 e 50 del DPCM 22 febbraio 2013; in particolare:

- Le chiavi di Certificazione e di Marcatura Temporale, ai sensi dell'art. 49, comma 4, del DPCM 22 febbraio 2013, sono generate in presenza del responsabile del servizio di certificazione e validazione temporale.

- La coppia di chiavi utilizzata per la validazione temporale è di lunghezza pari a 2048 bit e viene associata in maniera univoca al sistema di validazione temporale al momento della generazione.

Al fine di limitare il numero di marche temporali generate con la medesima coppia, le chiavi di Marcatura Temporale sono sostituite ed un nuovo Certificato emesso dopo non più di 3 (tre) mesi di utilizzazione, indipendentemente dalla durata del loro periodo di validità e senza revocare il corrispondente Certificato.
Il profilo dei Certificati di Marcatura Temporale è conforme alla Deliberazione CNIPA n. 45 del 21 maggio 2009.

6.2.4 Consegna della chiave privata al Richiedente

La chiave privata è contenuta all'interno del dispositivo: HSM in caso di firma remota, supporto fisico nel caso di token o smart card. Il Titolare, nel momento in cui riceve il Certificato diventa responsabile di quest'ultimo, così come della chiave privata che può essere utilizzata soltanto con il PIN consegnato, che deve essere custodito in maniera esclusiva.

6.3 Protezione della chiave privata e controlli ingegneristici sul modulo crittografico

Le coppie di chiavi utilizzate dalla CA per firmare i Certificati e le CRL sono memorizzate in un HSM (Hardware Security Module) di alta qualità.
L'HSM utilizzato da Namirial è Certificato al livello EAL4+ Common Criteria e qualificato ANSSI al massimo livello.

6.3.1 Algoritmi crittografici e lunghezza delle chiavi

Ai sensi dell'art. 3 della Deliberazione CNIPA n. 45 del 21 maggio 2009:

- nelle operazioni di firma è usato l'algoritmo RSA (Rivest-Shamir-Adleman);
- le chiavi usate dal Certificatore per firmare i Certificati hanno lunghezza almeno pari a 4096 bit;
- la lunghezza della chiave di sottoscrizione dei Titolari è pari almeno a 2048 bit.

6.3.2 Funzioni di HASH

Per la generazione dell'impronta viene utilizzata la funzione di hash SHA-256.

6.4 Altri aspetti relativi alla gestione della coppia di chiavi

Namirial usa in modo appropriato le chiavi private di firma della CA e non le utilizza oltre la fine del loro ciclo di vita.

In particolare:

- La chiave di firma della CA utilizzata per la generazione di Certificati e/o l'emissione di informazioni sullo stato di revoca, non viene utilizzata per nessun altro scopo;
- Le chiavi di firma della CA sono utilizzate solo all'interno di locali fisicamente sicuri;
- L'uso della chiave privata della CA è compatibile con l'algoritmo di hash, l'algoritmo di firma e la lunghezza della chiave di firma utilizzata per generare i Certificati, in linea con la sezione 6.3;
- Tutte le copie delle chiavi private di firma della CA saranno distrutte alla fine del loro ciclo di vita.

6.5 Dati di attivazione

I dati di attivazione consistono nel set necessario all'attivazione del processo di consegna del Certificato di sottoscrizione; le attività sono descritte nell'apposito paragrafo 4.4

6.6 Controlli di sicurezza informatica

I sistemi operativi utilizzati dalla CA per gestire i Certificati possiedono un elevato livello di sicurezza e seguono le procedure di hardening stabilite da Namirial. I compiti e le aree di responsabilità sono segregati al fine di minimizzare la possibilità di apportare modifiche non autorizzate o involontarie o abusare degli asset Namirial.
Gli eventi di accesso ai sistemi sono registrati, come descritto nella sezione relativa ai controlli fisici.
I componenti della rete locale, sia fisici che logici, sono mantenuti in un ambiente sicuro e le configurazioni sono periodicamente controllate per verificarne la conformità ai requisiti specificati da Namirial.
Sono implementati dei job che verificano il controllo dell'integrità del software della CA e della sua configurazione.
Sono previste strutture di monitoraggio continuo e alert per consentire a Namirial di rilevare, registrare e reagire tempestivamente a qualsiasi tentativo non autorizzato e/o irregolare di accesso alle proprie risorse.

6.7 Controlli di sicurezza sul ciclo di vita del processo

6.7.1 Controlli sugli asset

Namirial utilizza sistemi e prodotti affidabili protetti da modifiche e che garantiscono la sicurezza tecnica e l'affidabilità dei processi da essi supportati.

In particolare:

- Un'analisi dei requisiti di sicurezza viene effettuata durante la fase di progettazione e identificazione dei requisiti di qualsiasi progetto di sviluppo di sistemi intrapreso da Namirial;
- Le procedure di change management sono applicate a rilasci, modifiche e patch di emergenza di qualsiasi software operativo nonché a changes a livello di configurazione cui si applica la politica di sicurezza delle informazioni.
- L'integrità dei sistemi e degli asset Namirial è protetta da virus, software maligni e non autorizzati.
- Le procedure di gestione dei media sono definite e implementate al fine di proteggere questi da danni, furti, accessi non autorizzati, obsolescenza e deterioramento nel periodo di tempo in cui i record devono essere conservati.
- Le procedure organizzative sono definite e implementate al fine di gestire tutti i ruoli di fiducia e amministrativi che hanno un impatto sulla fornitura dei servizi.

6.7.2 Controlli sulla chiave privata

Al fine di emettere e gestire le chiavi CA in modo sicuro, Namirial utilizza HSM (Hardware Security Module), che:

- Sono a prova di manomissione e garantiscono la protezione delle chiavi secondo i livelli di sicurezza previsti dalla normativa e l'elevato standard tecnologico;
- impediscono qualsiasi tentativo non autorizzato di lettura, duplicazione, estrazione della chiave privata
- conserva la Chiave Privata per garantirne l'integrità per l'intero ciclo di vita;
- identifica gli operatori.

6.8 Controlli di network security

L'architettura di rete di Namirial è strutturata su più livelli in modo da creare ambienti di rete separati, indirizzati a host relativi a funzioni diverse e caratterizzati da diversi livelli di criticità.
La sicurezza degli accessi e del traffico di rete è garantita mediante l'applicazione di politiche di protezione implementate sui sistemi firewall dislocati su diversi livelli di rete.
Le richieste di implementazione di nuove regole sul firewall sono gestite attraverso una change request.
L'attivazione di regole che causano un alto livello di impatto, viene trattata con il Security Officer. La sicurezza della rete privata CA è realizzata non solo dai sistemi di protezione perimetrale descritti in precedenza, ma anche da una configurazione specifica che mantiene gli indirizzi interni come riservati. Le comunicazioni tra le stazioni di gestione e i sistemi sono protette per mezzo di strumenti che assicurano l'autenticazione tra le parti e la loro privacy.
I potenziali collegamenti remoti avvengono su un canale VPN criptato e richiedono l'autenticazione tramite Username, Password e un token di autenticazione (OTP).
La comunicazione tra i moduli applicativi della piattaforma PKI di Namirial avviene attraverso canali crittografici.

La comunicazione tra gli utenti che accedono ai servizi online avviene attraverso connessioni TLS/SSL con algoritmo SHA -256.
Il sistema implementato per gestire gli accessi degli utenti fornisce sia meccanismi AAA (autenticazione, autorizzazione, accesso) e di profilazione che la crittografia del canale di comunicazione con protocollo TLS/SSL.
Il sistema dovrebbe anche gestire gli accessi che provengono dai consulenti che lavorano sulla rete interna di Namirial.

6.9 Timestamping

Tutti i sistemi utilizzati dalla CA durante il flusso sono allineati con i riferimenti temporali UTC e sincronizzati tramite una fonte affidabile quali server NTP.

7. Policy, limiti d'uso e gestione dei Certificati

7.1 Profili dei Certificati

I Certificati sono conformi ai seguenti requisiti normativi:

- international standard ISO/IEC 9594-8:2005 [X.509 versione 3];
- specifiche pubbliche IETF RFC 5280 Management of Reliable Public Certificates;
- ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles (Part 1, 2, 3, 5).

La CA compila i campi dell'emittente e del soggetto di ogni Certificato emesso in seguito all'adozione dei requisiti, definiti sopra, in conformità con quanto dichiarato nel presente documento. Con l'emissione del Certificato, la CA dichiara di aver seguito la procedura descritta nel documento per dimostrare che, alla data di emissione del Certificato, tutte le informazioni relative al soggetto erano accurate.
Le sezioni seguenti descrivono i principali attributi normalmente inclusi in ogni Certificato Qualificato emesso da Namirial. Qualora il Richiedente richieda un nuovo tipo di attributi, non inclusi di seguito, Namirial li imposterà di conseguenza, a condizione che il nuovo set di attributi sia conforme alle specifiche di cui sopra.
Come richiesto dalla normativa italiana, l'emissione di Certificati di Firma Qualificata o di Marca Temporale avviene utilizzando direttamente i seguenti Certificati CA root:

Nome CA Root	Scopo	Note
Namirial Qualified eSignature	Emissione certificati per firma digitale	Certificato CA Root
Namirial CA Firma Qualificata	Emissione certificati per firma digitale	Certificato CA Root
Namirial EU Qualified eSignature	Emissione certificati qualificati per firma elettronica	Certificato CA Root
Namirial EU Qualified CA	Emissione certificati qualificati per firma elettronica e sigillo elettronico	Certificato CA Root
Namirial Time Stamping Authority	Emissione certificati per marca temporale	Certificato CA Root

Namirial CA TSA	Emissione certificati per marca temporale	Certificato CA Root

Tabella 4: Certificate profile

7.1.1 Namirial EU Qualified e-Signature

Version	Version 3
Serial Number	21 0d 6c b1 7c 11 0b 9b
Signature	sha256, RSA
Issuer (ETSI 319 412-2 par. 4.2.3.1)	Issuer DN: **countryName**: "IT" **organizationName**: "Namirial S.p.A." **organizationalUnit:** "Namirial Trust Service Provider" **organizationIdentifier**: "VATIT- 02046570426" **commonName**: "Namirial EU Qualified eSignature"
Validity Period	20 Years (expire 20 years from the date of issue)
Subject	Equal to Issuer
SubjectPublicKeyInfo	Public Key 4096 bit Algorithm: RSA
Extentions	
Subject Key Identifier	30 45 db 26 02 3d bf 0d 9a d8 b8 10 ea 7c cd a4 ae 8e 5c 27
Authority Key Identifier	30 45 db 26 02 3d bf 0d 9a d8 b8 10 ea 7c cd a4 ae 8e 5c 27
Certificate Policies	Not critical Policy OID, 1.3.6.1.4.1.36203.1.1 Cp: URL: https://docs.namirialtsp.com/
crlDistributionPoint	Not critical http://crl.namirialtsp.com/QES4K.crl
Basic Constraint (critical)	Critical Subject Type: CA Path Length Constraint: no constraint
KeyUsage (critical)	CertSign, cRLSign

Table 1 - Namirial EU qualified e-signature

7.1.2 Namirial Firma Qualificata

Version	Version 3
Serial Number	6E E8 2F B2 FF 76 2F 06
Signature	sha256, RSA
Issuer (ETSI 319 412-2 par. 4.2.3.1)	Issuer DN: **countryName**: "IT" **organizationName**: "Namirial S.p.A." organizationalUnit: "Namirial Trust Service Provider" **commonName**: " Namirial Qualified e-Signature"
Validity Period	20 Years (expire 20 years from the date of issue)
Subject	Equal to Issuer
SubjectPublicKeyInfo	Public Key 2048 bit Algorithm: RSA
Extentions	
Subject Key Identifier	0b a4 b2 bb 27 39 c1 e1 09 d3 77 6c b8 75 e1 67 8d e3 22 fe
Authority Key Identifier	0b a4 b2 bb 27 39 c1 e1 09 d3 77 6c b8 75 e1 67 8d e3 22 fe
Certificate Policies	Not critical Policy OID, 1.3.6.1.4.1.36203.1.1 Cp: URL: https://docs.namirialtsp.com/
crlDistributionPoint	Not critical http://crl.namirialtsp.com/QES.crl
Basic Constraint (critical)	Critical Subject Type: CA Path Length Constraint: no constraint
KeyUsage (critical)	CertSign, cRLSign

Table 2 - Namirial qualified e-signature

7.1.3 Namirial CA Firma Qualificata

Version	Version 3
Serial Number	41 58 c1 3a 49 d2 98 19
Signature	sha256, RSA
Issuer (ETSI 319 412-2 par. 4.2.3.1)	Issuer DN: **countryName**: "IT" **organizationName**: "Namirial S.p.A./02046570426"

	organizationalUnit: “Certification Authority” **commonName**: “ Namirial CA Firma Qualificata”
Validity Period	20 Years (expire 20 years from the date of issue)
Subject	Equal to Issuer
SubjectPublicKeyInfo	Public Key 2048 bit Algorithm: RSA
Extentions	
Subject Key Identifier	63 fd ed e6 8c 62 47 48 cf ea 09 41 73 76 11 e2 64 62 7b 10
Authority Key Identifier	63 fd ed e6 8c 62 47 48 cf ea 09 41 73 76 11 e2 64 62 7b 10
Certificate Policies	Not critical Policy OID, 2.5.29.32.0
crlDistributionPoint	Not critical http://crl.firmacerta.it/FirmaCertaQualificata1.crl
Basic Constraint (critical)	Critical Subject Type: CA Path Length Constraint: no constraint
KeyUsage (critical)	CertSign, cRLSign

Table 3 - Namirial CA firma qualificata

7.1.4 Namirial EU Qualified CA

Version	Version 3
Serial Number	39 61 62 D9 E5 04 83 A3
Signature	sha256, RSA
Issuer (ETSI 319 412-2 par. 4.2.3.1)	Issuer DN: **countryName**: “IT” **organizationName**: “Namirial S.p.A.” organizationalUnit: “Trust Service Provider” **commonName**: “ Namirial EU Qualified CA”
Validity Period	20 Years (expire 20 years from the date of issue)
Subject	Equal to Issuer
SubjectPublicKeyInfo	Public Key 4096 bit Algorithm: RSA
Extentions	

Subject Key Identifier	63 B8 CD B8 49 52 E5 E7 09 7B 57 8C FB 7A 41 0E 41 AA 78 59
Authority Key Identifier	63 B8 CD B8 49 52 E5 E7 09 7B 57 8C FB 7A 41 0E 41 AA 78 59
Certificate Policies	Not critical Policy OID 1.3.6.1.4.1.36203.1.1
crlDistributionPoint	Not critical http://crl.namirialtsp.com/CA4K.crl
Basic Constraint (critical)	Critical Subject Type: CA Path Length Constraint: no constraint
KeyUsage (critical)	CertSign, cRLSign

Table 4 - Namirial EU Qualified CA

7.2 Registro dei Certificati

Il registro dei Certificati contiene:

- tutti i Certificati emessi dal Certificatore;
- la lista dei Certificati sospesi e revocati (CRL).

7.3 Profilo CRL

La CRL è conforme alle specifiche pubbliche RFC 5280.

Version	2
signature	sha256withRSA
Issuer	CA DN
Thisupdate	This field indicates the issue date of this CRL.
Nextupdate	The date by which the next CRL will be issued. The next CRL could be issued before the indicated date, but it will not be issued any later than the indicated date.
reevokedCertificate	List of revoked certificates' serial numbers
CRL.Extensions	CRLNumber, ExpiredCertsOnCRL and Authority Key Identifier
signatureAlgorithm	sha256withRSA
Signature Valure	Signature computed on the hash of the DER encoding of CertList.

Table 5 - CRL profile

7.4 Profilo OCSP

Il protocollo OCSP è conforme alle specifiche pubbliche RFC 6960.
Di seguito in dettaglio la lista dei campi contenuti all'interno delle response OCSP fornite dal Namirial OCSP Responder.

responseStatus	Choice of Successful (0), malformed (1), internalError (2), tryLater (3), sigRequired (5), unauthorized (6) Related to state and/or configuration of the Service (as for Rfc 6960)
Basic Response	
Version	1 (0x0)
Responder ID	SHA-1 of the Reponder's Public Key (excluding the tag and length fields)
ProducedAt	GeneralizedTime of production of the response (UTC). The time at which the OCSP responder signed this response.
SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Responses	Only one response per certificate
CertID.hashAlgorithm	SHA-1 160 bit
CertID.issuerNameHash	Hash (SHA-1) of issuer's DN
CertID.issuerKeyHash	Hash (SHA-1) of issuer's public key
CertID.serialNumber	CertificateSerialNumber
Cert Status	Choise between: Good[0], Revoked[1], Unknown[2]
Cert Status.RevokedInfo	revocationTime = The time at which the certificate was revoked or placed on hold. revocationReason = The reason for revocation of certificate
thisUpdate	The most recent time at which the status being indicated is known by the responder to have been correct.
Response.Extensions	OCSP nonce
signatureAlgorithm	sha256withRSA
Signature	Signature computed on the hash of the DER encoding of ResponseData.
Certs	OCSP Responder's Certificate

	CA's Certificate

Table 6 - OCSP profile

7.5 Accesso al registro dei Certificati

La copia di riferimento del registro dei Certificati è accessibile esclusivamente dal sistema di generazione dei Certificati. La pubblicazione delle informazioni sulle copie operative del registro dei Certificati è consentita solamente al Certificatore. Tali informazioni sono pubblicamente accessibili in sola lettura e tramite il protocollo http.
Ai sensi dell'art. 42 comma 3 del DPCM 22 febbraio 2013 il Certificatore rende inoltre accessibile al seguente URL copia della lista, sottoscritta dall'Agenzia, dei Certificati relativi alle chiavi di certificazione di cui all'articolo 43, comma 1, lettera e) del DPCM di cui in precedenza:

https://cms.firmacerta.it/Certificatori/Certificatori.zip.p7m

7.6 Gestione del registro dei Certificati

La copia di riferimento del registro dei Certificati è gestita dal Certificatore, non è accessibile dall'esterno e contiene tutti i Certificati Qualificati e le liste di revoca emessi dal Certificatore.
Tutte le operazioni che modificano i dati all'interno del registro sono automaticamente riportate nel Giornale di Controllo.
Il registro è aggiornato all'emissione di ogni Certificato Qualificato e alla pubblicazione della lista di revoca (CRL).
Le liste di revoca dei Certificati (CRL) sono accessibili pubblicamente in sola lettura e contengono i Certificati di sottoscrizione revocati o sospesi. La pubblicazione delle liste di revoca è aggiornata in modo sincrono ad ogni aggiornamento del registro dei Certificati revocati o sospesi.

7.7 Archiviazione dei Certificati Qualificati e di Marcatura Temporale

I Certificati Qualificati e quelli relativi alle chiavi di Marcatura Temporale sono archiviati e conservati per 20 (venti) anni dalla emissione.
Le chiavi private di firma di cui sia scaduto il Certificato non possono più essere utilizzate.

8. Audit e conformità

Namirial è un Trust Service Provider deputato al rilascio della Firma Qualificata e accreditato da un organismo di certificazione, a sua volta accreditato da Accredia. Il rapporto di valutazione della conformità viene inviato ad AgID.
Di conseguenza, Namirial è soggetta ad una valutazione di conformità ("sorveglianza") da parte della stessa Agenzia ed è tenuta ad effettuare ispezioni interne periodiche.

8.1 Frequenza e circostanze della valutazione di conformità

La funzione di audit di Namirial è responsabile degli audit interni sui servizi di Firma Digitale. Si occupa di verificare che i processi siano conformi ai requisiti di legge e ad a regolamenti e procedure aziendali. L'audit interno viene effettuato almeno una volta all'anno. L'audit di terza parte invece, eseguito da un organismo di certificazione accreditato da Accredia, viene effettuato con periodicità annuale.

8.2 Identità e qualifica di chi effettua il controllo

Gli audit di conformità sono svolti da Bureau Veritas Italia.
Gli audit interni sono invece a carico della funzione aziendale preposta, che si serve di dipendenti opportunamente qualificati.

8.3 Rapporti tra Namirial e organismo di certificazione

Non esiste alcun rapporto tra Namirial e l'ente di certificazione che possa in qualche modo influenzare i risultati degli audit a favore di Namirial.

8.4 Perimetro oggetto di valutazione

L'organismo di certificazione esegue la valutazione della conformità delle attività Namirial, supervisionate da AgID, che operano nel rispetto del Regolamento UE 910/2014, noto come "eIDAS-Electronic Identification Authentication and Signature".
L'audit interno è principalmente volto a verificare l'integrità del Giornale di Controllo, e il rispetto delle procedure operative della Certification Authority.

8.5 Azioni derivanti da non conformità

In caso di non conformità, Namirial adotta le azioni correttive necessarie tracciate e misurate fino alla risoluzione.

8.6 Comunicazione dei risultati

I risultati dell'audit, effettuati organismo di certificazione, sono condivisi con la Certification Authority attraverso un rapporto di valutazione della conformità. Il risultato dell'audit interno viene comunicato alla Direzione e al Responsabile della struttura organizzativa incaricata della fornitura del servizio.

9. Altri aspetti legali e di business

9.1 Tariffe

Le tariffe massime del servizio sono pubblicate sullo Shop del Certificatore.
Condizioni diverse possono essere negoziate su base personalizzata, a seconda dei volumi richiesti.

9.2 Responsabilità finanziaria

Namirial ha sottoscritto un'assicurazione adeguata a coprire i rischi dell'attività e gli eventuali danni derivanti dal servizio di certificazione.

9.3 Responsabilità del Titolare

Il Titolare ha la responsabilità di fornire informazioni certe, veritiere e riconducibili alla propria identità. È chiamato altresì al rispetto delle modalità previste per l'emissione e la custodia delle credenziali, nonché all'attenta lettura del materiale informativo messo a disposizione della CA, di cui il presente manuale è parte. Tale soggetto è inoltre tenuto a seguire in maniera scrupolosa le indicazioni fornite dal Certificatore.
Il Richiedente, se presente, deve fornire alla CA informazioni certe, veritiere e riconducibili all'identità per conto del quale sta richiedendo il Certificato. Si dovrà inoltre far carico di informare il Titolare circa gli obblighi previsti per la custodia delle credenziali,

9.4 Responsabilità della CA e limitazioni agli indennizzi

9.4.1 Limitazioni di responsabilità del Certificatore

Il Certificatore è responsabile, verso i Titolari, per l'adempimento degli obblighi di legge derivanti dalle attività previste dal D.Lgs. 82/2005, dalla Circolare CNIPA del 6 settembre 2005, dal DPCM 22 febbraio 2013, dal Regolamento eIDAS, dal DPR 445/2000, dalla Deliberazione CNIPA 45/2009 e dalla Determinazione Commissariale n.69/2010 DigitPA e successive modifiche ed integrazioni.

Il Certificatore, ove previsto, mette a disposizione del Titolare un apposito kit configurato secondo due modalità alternative:

- Dispositivo sicuro di firma (smart card, Token SIM USB o Micro SD) completo di Certificato di firma e del software, accuratamente testato, per l'apposizione e la verifica delle firme qualificate.
- Dispositivo sicuro di firma (smart card, Token SIM USB o Micro SD) non personalizzato (senza chiavi di sottoscrizione), procedura di personalizzazione del dispositivo e software, per l'apposizione e la verifica delle firme qualificate (art 7 -11)

Il Certificatore non assume responsabilità:

- per l'uso improprio dei Certificati emessi;
- per le conseguenze derivanti dalla non conoscenza o dal mancato rispetto, da parte del Titolare, delle procedure e delle modalità operative indicate nel presente documento;
- per il mancato adempimento degli obblighi previsti a suo carico dovuto a cause ad esso non imputabili;

9.4.1.1. Limitazioni e Indennizzi

Ai sensi dell'art. 57, comma 2 del DPCM 22 febbraio 2013 il Certificatore ha stipulato polizza assicurativa per la copertura dei rischi dell'attività e dei danni a tutte le parti (Titolari, Terzi Interessati, Destinatari) non superiore ai massimali di seguito indicati:

- € 150.000 per singolo sinistro per un totale di € 1.500.000 per anno assicurativo per tutte le perdite patrimoniali derivanti da tutte le richieste di risarcimento presentate contro il Certificatore per tutte le coperture assicurative combinate.

9.5 Confidenzialità e trattamento dei dati personali

9.5.1 Protezione dei dati personali

Di seguito vengono descritte le procedure e le modalità operative che Namirial S.p.A., in qualità di Titolare del trattamento dei dati personali, adotta nello svolgimento della propria attività. Le informazioni personali, concernenti i Titolari dei Certificati e, più in generale i clienti del servizio erogato vengono trattate, conservate e protette in conformità a quanto previsto nel Regolamento europeo 679/2016 in materia di protezione dei dati personali.

9.5.2 Tutela e diritti degli interessati

Namirial S.p.A. garantisce la tutela degli interessati, in ottemperanza al Regolamento europeo 679/2016 in materia di protezione dei dati personali. In particolare, fornisce agli interessati tutte le informazioni necessarie, in relazione al diritto di accesso ai dati personali ed agli usi degli stessi, consentiti dalla legge.
L'accesso ai propri dati da parte degli interessati è consentito tramite richiesta scritta, a mezzo del format scaricabile dal sito web di Namirial ww.namirial.com da far pervenire al responsabile per la protezione dei dati anche tramite e-mail all'indirizzo dpo@namirial.comche provvederà ad evadere la richiesta senza ingiustificato ritardo.
Gli interessati devono prestare consenso scritto al trattamento dei propri dati da parte di Namirial S.p.A.

9.5.3 Modalità del trattamento

Tutte le informazioni personali, acquisite durante l'erogazione dei servizi, vengono trattate da Namirial che adotta le misure di sicurezza, descritte all'interno del presente manuale allo scopo di prevenirne la perdita, evitarne usi illeciti o accessi da parte di personale non espressamente autorizzato.
I dati in formato elettronico vengono conservati in appositi data server adibiti allo scopo e su supporti ottici all'interno di armadi protetti.
Namirial S.p.A. si riserva l'opportunità di conservare i dati cartacei presso la propria sede centrale, all'interno di archivi cartacei cui hanno accesso solo gli incaricati espressamente autorizzati.

9.5.4 Finalità del trattamento

I dati personali vengono acquisiti in osservanza alle finalità esplicitate nell'informativa fornita al Richiedente durante le fasi di richiesta del Certificato. L'informativa è anche pubblicata su https://docs.namirialtsp.com/privacy/.
Di seguito, elencate, le finalità del trattamento.

- gestione del rapporto contrattuale;
- eventuali controlli sulla qualità del servizio e sulla sicurezza del sistema;
- attività di natura commerciale, effettuata tramite invio di informative legate alla emissione di prodotti e/o servizi analoghi o direttamente connessi ai servizi di Certificazione e Marca Temporale.

L'interessato ha la possibilità di opporsi al trattamento dei dati personali, avente ad oggetto tale tipologia di comunicazioni.

9.5.5 Altre forme di utilizzo dei dati

I dati personali possono essere usati con finalità diverse rispetto alla fornitura dei servizi descritti dal presente manuale e possono essere comunicati a soggetti pubblici, quali forze dell'ordine, autorità pubbliche e autorità giudiziarie, qualora gli stessi soggetti ne facciano richiesta per motivi di ordine pubblico e nel rispetto delle disposizioni di legge per la sicurezza e difesa dello Stato, la prevenzione, l'accertamento e/o la repressione dei reati.

9.5.6 Sicurezza dei dati

In ottemperanza normativa vigente, Namirial S.p.A. adotta tutte le misure di sicurezza necessarie al fine di ridurre al minimo:

- i rischi di distruzione o perdita, anche accidentale, dei dati;
- i rischi di danneggiamento di risorse hardware sulle quali siano memorizzati i dati;
- i rischi di danneggiamento ai locali nei quali siano custoditi i dati;
- l'accesso non autorizzato ai dati;

- le attività di trattamento non consentite dalla legge o dai regolamenti aziendali

Attraverso le misure di sicurezza adottate da Namirial vengono inoltre garantite:

- l'integrità e la salvaguardia dei dati, contro manomissioni o modifiche da parte di soggetti non autorizzati
- la disponibilità dei dati e la loro conseguente fruibilità;
- la riservatezza dei dati ovvero la garanzia che alle informazioni abbiano accesso le sole persone autorizzate.

9.6 Archivi contenenti dati personali

L'archivio contenente i dati personali è il database di registrazione.
Gli archivi sopra elencati sono gestiti dal responsabile della registrazione e sono adeguatamente protetti da accessi non autorizzati, in conformità a quanto previsto dal GDPR e successivi aggiornamenti

9.7 Diritti di proprietà intellettuale

Questo documento è di proprietà di Namirial, che si riserva tutti i diritti relativi ad esso. Il proprietario del Certificato mantiene tutti i diritti sul proprio marchio (brand name) e sul suo nome di dominio. In relazione alle proprietà di altri dati e informazioni si applica la legge in vigore.

9.8 Obblighi e garanzie

9.8.1 Certification Authority

La CA è obbligata a:

- Operare in conformità con questo documento;
- Identificare Richiedenti e Titolari come descritto in questo documento;
- Emettere e gestire i Certificati come descritto in questo documento;
- Fornire un servizio efficiente di sospensione o revoca dei Certificati;
- Assicurarsi che il proprietario possieda, al momento dell'emissione del Certificato, la chiave privata corrispondente;
- Segnalare tempestivamente l'eventuale compromissione della chiave privata;
- Fornire informazioni chiare e complete sulle procedure e sui requisiti del servizio;
- Fornire una copia di questo documento a chiunque ne faccia richiesta;
- Garantire che la fornitura di servizi di firma digitale sia accessibile alle persone con disabilità;
- Garantire un trattamento dei dati personali conforme alla normativa vigente;
- Garantire la disponibilità del servizio, salvo in caso di attività di manutenzione programmata, preventivamente comunicata;
- Fornire un servizio di informazione efficiente e affidabile sullo stato dei Certificati.

9.8.2 Registration Authority

La Registration Authority tratta i dati personali dell'interessato con la massima riservatezza e in conformità a quanto previsto dal GDPR.

9.8.3 Richiedenti o Titolari

Il Richiedente o il Titolare ha l'obbligo di:

- Leggere, comprendere e accettare completamente questo documento;
- Richiedere il Certificato fornito da questo documento;
- Generare in modo sicuro la coppia di chiavi pubbliche e private, utilizzando un sistema affidabile;
- Fornire alla CA informazioni accurate e veritiere nella fase di registrazione;
- Adottare misure tecniche e organizzative volte a prevenire la compromissione della chiave privata;
- Garantire la privacy dei codici riservati ricevuti dalla CA;
- Richiedere la sospensione immediata del Certificato in caso di sospetta o confermata compromissione della chiave privata;
- Richiedere immediatamente la revoca del Certificato nel caso in cui una o più informazioni contenute nel Certificato perdano validità;
- In seguito all'emissione e fino alla scadenza o alla revoca del Certificato, comunicare tempestivamente alla CA ogni modifica delle informazioni fornite in fase di richiesta;

9.8.4 Utenti finali

Gli utenti finali, quindi tutte le entità (diverse dal Richiedente o dal Titolare) che fanno affidamento sui Certificati emessi ai sensi del presente documento, hanno l'obbligo di:

- Fare in modo di ottenere informazioni sufficienti sul funzionamento dei Certificati e della PKI;
- controllare lo stato dei Certificati emessi da Namirial sulla base del presente documento;
- fare affidamento su un Certificato solo se non è scaduto, sospeso o revocato.

9.9 Limitazioni di garanzia

Si applica quanto descritto all’interno del documento Trust Service Practice Statement.

9.10 Limitazioni di indennizzo

Si applica quanto descritto all’interno del documento Trust Service Practice Statement.

9.11 Indennizzi

Si applica quanto descritto all’interno del documento Trust Service Practice Statement.

9.12 Termini e risoluzione

Si applica quanto descritto all'interno del documento Trust Service Practice Statement.

9.13 Comunicazioni

Si applica quanto descritto all'interno del documento Trust Service Practice Statement.

9.14 Procedure di risoluzione delle controversie

Si applica quanto descritto all'interno del documento Trust Service Practice Statement.

9.15 Foro competente

Si applica quanto descritto all'interno del documento Trust Service Practice Statement.

9.16 Legge applicabile

Si applica quanto descritto all'interno del documento Trust Service Practice Statement.

Appendice A: Strumenti e modalità per l'apposizione e la verifica della firma digitale

Gli strumenti messi a disposizione dal Certificatore consentono di effettuare firme di tipo PAdES, CAdES e XAdES. Maggiori informazioni sulle tipologie di firme utilizzabili possono essere reperite sul sito http://www.agid.gov.it/.

Per l'apposizione della firma digitale sono previste due modalità:

- firma con dispositivo di firma personale (es. smartcard, token USB o simile),
- firma con procedura automatica/remota basata sull'impiego di HSM.

Nei paragrafi che seguono si riportano le modalità operative per entrambi i casi.

Firma con dispositivo di firma personale

Namirial mette gratuitamente a disposizione degli utenti un software denominato "FirmaCerta" che consente, con facilità d'uso, di eseguire tutte le operazioni relative alla firma digitale. Nello specifico il software consente, per ogni singolo file:

- La firma digitale;
- La marcatura temporale;
- La verifica della firma e della marca temporale;
- La controfirma di un file (validazione);
- La firma grafometrica.

Tra le funzionalità offerte dal prodotto "FirmaCerta" vi è inoltre la possibilità di:

- firmare contemporaneamente grandi volumi di documenti digitali, come fatture, polizze, ricevute di pagamenti, bonifici e qualsiasi altro documento digitale;
- firmare i documenti PDF mantenendo il formato originale;
- scegliere il dispositivo hardware col quale si desidera apporre la firma (Smart Card, Token);
- apporre/associare una marca temporale ad un documento o ad una firma (Grafometrica);
- selezionare i file con il drag & drop di uno o più file all'interno della stessa finestra di firma;
- firmare i documenti PDF protetti da password, previa conoscenza della stessa.

I prerequisiti hardware e software nonché tutte le indicazioni per l'installazione del prodotto "FirmaCerta" sono riportate nella "Guida rapida all'utilizzo" del software, reperibile al seguente URL:

http://www.firmacerta.it/manuali.php

Nel documento, che è parte integrante del presente Manuale Operativo, sono riportate le modalità operative per effettuare la generazione e la verifica della firma digitale.
Alcuni formati di documenti permettono di inserire del codice eseguibile (macro o comandi) all'interno del documento senza che questo ne alteri la struttura binaria e tali da attivare funzionalità che possono modificare gli atti, i fatti o i dati rappresentati nel documento medesimo. Si ricorda che i file firmati digitalmente che contengono tali strutture non producono gli effetti di cui all'articolo 21, comma 2 del CAD ed è cura del Titolare assicurarsi, tramite le funzionalità tipiche di ciascun prodotto, dell'assenza di tali codici eseguibili.
In Appendice C sono riportate le modalità operative, in riferimento ad alcuni formati di larga diffusione, per accertarsi che il documento non contenga macroistruzioni o codici eseguibili.

Firma con applicazioni di firma automatica

L'utente utilizza un'applicazione "client" di firma fornita dal Certificatore o dal Cliente (es. impresa, banca, ente pubblico, ecc.) che eroga servizi applicativi ad utenti interni o esterni. Le specifiche modalità per l'esecuzione della firma dipendono quindi dalla particolare applicazione client usata dagli utenti e vengono all'occorrenza descritte caso per caso dagli addendum al manuale operativo.
La soluzione fornita dal Certificatore è composta da due componenti:

- **HSM ed il server SignEngine (di seguito SE) che lo controlla e lo pilota.** SE è responsabile della firma a basso livello degli hash dei documenti.
- **Il server SignWebServices (di seguito SWS).** È la componente capace di apporre e verificare le firme ad un alto livello di astrazione. Si integra con i sistemi del cliente (custom o legacy). Necessita di comunicare con la componente SE, ma può essere dislocata altrove. SWS esegue l'imbustamento nei vari formati supportati e calcola gli hash da far firmare a SE.

Si configurano pertanto due differenti scenari di utilizzo:

- **HSM presso il CED del cliente.** Tale configurazione è preferibile nel caso si debba produrre un numero considerevole di firme e garantisce maggiori risultati in termini di performance poiché l'HSM è dedicato e non ci sono ritardi di rete apprezzabili in quanto tutte le comunicazioni avvengono su LAN. In questo scenario sia la componente SE che SWS sono istallate presso il cliente.
- **HSM presso Namirial.** Con questa configurazione il cliente si limita ad effettuare l'integrazione tra i suoi sistemi e la componente SWS, disinteressandosi dell'acquisto e dell'esercizio dell'HSM. In questo scenario il cliente necessita della sola componente SWS o dell'applicazione di firma remota fornita dal Certificatore.

Il sistema di firma automatica, basato su HSM, può essere quindi ospitato presso il data center del Certificatore oppure presso il data center del Cliente; nel secondo caso, il Cliente deve rispettare i requisiti di sicurezza fisica, logica, operativa e gestionale indicati dal Certificatore, il quale svolgerà verifiche periodiche sul rispetto di tali requisiti in conformità all'articolo 3, comma 5 del DPCM.
Le componenti *SE* e *SWS* stabiliscono autonomamente connessioni sicure sempre protette tramite i protocolli TLS/SSL, con autenticazione del server e cifratura della sessione con chiavi simmetriche di almeno 128 bit e, in conformità all'art. 42 comma 6 del DPCM, non consentono al Certificatore di conoscere gli atti o fatti rappresentati nel documento informatico oggetto del processo di sottoscrizione o verifica.
La richiesta di firma proveniente dal client è autenticata con username e password. Gli utenti accedono al server esclusivamente attraverso una rete locale (LAN) non raggiungibile da Internet e il Certificato di firma contiene le opportune limitazioni d'uso.

Firma con applicazioni di firma remota

Per l'apposizione della firma in modalità remota, sarà possibile utilizzare applicazioni distribuite dal Certificatore o dal Cliente (es. impresa, banca, ente pubblico, ecc) che eroga servizi applicativi ad utenti interni o esterni. Le specifiche modalità per l'esecuzione della firma dipendono quindi dalla particolare applicazione usata dagli utenti e vengono all'occorrenza descritte caso per caso dagli addendum al manuale operativo. La richiesta di firma proveniente dall'utente è sempre autenticata con due fattori. La modalità standard si basa sull'uso di un PIN statico (primo fattore) accompagnato da una password dinamica OTP (One-Time Password) che può essere, a seconda dei casi:

- token mobile
- token SMS
- token fisico

Il Certificatore mette a disposizione appositi strumenti desktop, web e mobile per la firma e la verifica.

In particolare *FirmaCerta* è un'applicazione desktop installabile su postazioni di lavoro dotate di sistema operativo Microsoft Windows. I prerequisiti hardware e software nonché tutte le indicazioni per l'installazione del prodotto "FirmaCerta" sono riportate nella "Guida rapida all'utilizzo" del software, reperibile al seguente URL:

http://www.firmacerta.it/manuali.php

Nel documento, che è parte integrante del presente Manuale Operativo, sono riportate le modalità operative per effettuare la generazione e la verifica della firma digitale.

FirmaCertaMobile è un'applicazione mobile, sviluppata dal Certificatore, installabile su dispositivi dotati di sistema operativo Android e IOS;

Viene inoltre fornita un'applicazione web utilizzabile per la firma e la verifica delle firme mediante i browser comunemente usati.
In ogni caso l'apposizione della firma richiederà che l'utente inserisca i seguenti codici:

- Codice Dispositivo Virtuale5
- PIN6
- OTP

Il Certificatore non può entrare in alcun modo a conoscenza o avere la possibilità di modificare il codice PIN. Sarà cura del Titolare gestire detto codice, senza il quale il Certificato associato non potrà essere utilizzato per l'apposizione di nuove firme.
In caso non si disponga più del codice *PIN* al Titolare è consigliato di procedere immediatamente alla sospensione del Certificato associato, secondo la procedura descritta al Paragrafo 4.13.2.

Si precisa inoltre che le applicazioni server utilizzate nell'ambito del servizio di firma remota adottano specifiche misure di sicurezza, in conformità all'art. 42 comma 6 del DPCM, e non consentono al Certificatore di conoscere gli atti o fatti rappresentati nel documento informatico oggetto del processo di sottoscrizione o verifica.

Modalità per l'apposizione e la definizione del Riferimento Temporale

L'emissione della marca temporale, richiesta dal Titolare del Certificato Qualificato è ottenuta mediante un software fornito dal Certificatore ed installato sul computer del Titolare, ed il servizio web è raggiungibile tramite internet con protocollo sicuro.
Il processo di marcatura è il seguente:

- il Titolare, mediante il software fornito con il kit, produce e firma la richiesta di marcatura temporale del documento informatico,
- La richiesta è inoltrata al Certificatore con protocollo sicuro (HTTPS),
- il Certificatore verifica la richiesta e le credenziali del Titolare,
- il Certificatore genera la marca temporale, con un sistema ad alta affidabilità che coincide con il momento della sua generazione, con una differenza non superiore ad un minuto secondo rispetto alla scala di tempo UTC (IEN).
- la marcatura viene consegnata al Titolare, in modalità sicura, per l'utilizzo.

L'impronta dell'evidenza informatica è calcolata utilizzando la funzione di hash SHA-256.

[5] Tale informazione è presente all'interno del modulo sottoscritto dal Titolare.
[6] Impostato dal Titolare in fase di generazione delle chiavi.

Nel caso in cui il sistema di marcatura temporale (TSA) riceva una richiesta non conforme viene restituito un messaggio d'errore.

Archiviazione e validità delle Marche Temporali

Tutte le marche temporali emesse dal sistema di validazione sono conservate in un apposito archivio digitale non modificabile.
Le marche sono conservate per 20 (venti) anni dalla data di emissione ed hanno validità per l'intero periodo di conservazione.

Precisone del Riferimento Temporale

Durante la generazione della marca temporale il server della TSA utilizza la data e l'ora dal clock del sistema, mantenuto allineato con l'ora UTC (Tempo Universale Coordinato) mediante due sistemi di sincronizzazione:

- una sonda esterna connessa al sistema della rete satellitare GPS,
- il servizio NTP messo a disposizione da INRIM.

L’accuratezza del sistema di riferimento temporale è pari a 1 secondo. La tolleranza, come richiesto dalla normativa vigente, non è mai superiore al minuto secondo rispetto alla scala di tempo UTC (IEN).

Appendice B – Namirial Certificate Policy

Certificate Policies

Il Certificatore utilizza i seguenti Object Identifier, (OID) afferenti al proprio Private Enterprise Number:

1.3.6.1.4.1.36203	Namirial S.p.A.
1.3.6.1.4.1.36203.1	CA FirmaQualificata
1.3.6.1.4.1.36203.1.1	Policy CA FirmaQualificata
1.3.6.1.4.1.36203.2	CA TSA
1.3.6.1.4.1.36203.2.1	Policy CA TSA
1.3.6.1.4.1.36203.4	CA Autenticazione
1.3.6.1.4.1.36203.4.1	Policy CA Autenticazione

Tabella 5: Namirial CA Object Identifier

I Certificati emessi secondo le regole del presente documento sono identificati con i seguenti Object Identifier, (OID):

1.3.6.1.4.1.36203.1.1.1	Policy per certificati associati ai server di marcatura temporale (utilizzata fino a Gennaio 2014). La policy identifica emissioni di marche temporali conformi allo standard RFC 3161
1.3.6.1.4.1.36203.1.1.2	Policy per certificati qualificati associati a dispositivo sicuro per la creazione della firma mediante procedura manuale.
1.3.6.1.4.1.36203.1.1.3	Policy per certificati qualificati associati ad apparato sicuro per la creazione della firma mediante procedura automatica. User Notice: Il presente certificato è valido solo per firme apposte con procedura automatica. This certificate may only be used for unattended/automated digital signatures.
1.3.6.1.4.1.36203.1.1.4	Policy per certificati associati ai server OCSP relativi ai certificati di Sottoscrizione.
1.3.6.1.4.1.36203.1.1.5	Policy per certificati qualificati associati ad apparato sicuro per la creazione della firma mediante procedura remota.
1.3.6.1.4.1.36203.1.2.1	Policy per certificati qualificati emessi a legal person la cui chiave privata non risiede in un Qualified Seal Creation Device

1.3.6.1.4.1.36203.1.2.3	Policy per certificati qualificati emessi a legal person la cui chiave privata risiede un Qualified Seal Creation Device
1.3.6.1.4.1.36203.2.1.1	Policy per certificati associati ai server di marcatura temporale (utilizzata da Gennaio 2014). La policy identifica emissioni di marche temporali conformi allo standard RFC 3161, al Regolamento eIDAS e allo standard ETSI EN 319 401e successive modificazioni.
1.3.6.1.4.1.36203.2.1.2	Policy per certificati usati per l'emissione di marche temporali qualificate. La policy identifica emissioni di marche temporali conformi allo standard RFC 3161, alRegolamento eIDAS, agli standard ETSI EN 319 401 e ETSI EN 319 421e successive modificazioni.
1.3.6.1.4.1.36203.4.1.2	Policy per Certificati dia.
1.3.6.1.4.1.36203.4.1.4	Policy per certificati associati ai server OCSP relativi ai certificati di autenticazione.

Tabella 6: Object Identifier dei Certificati emessi da Namirial CA

QCP-l-qscd Policy for EU qualified certificate issued to a legal person where the private key related to the certificated public key resides in a QSCD

Version	Version 3
Serial Number	Serial number of the certificates
Signature Algorithm	Sha256, RSA
Issuer	CA Dname
Validity Period	Max 6 Years
Subject (ETSI 319 412-3) (ETSI 319 412-1)	**countryName (OID 2.5.4.6):** *countryName contains the ISO 3166 country code in which the subject (legal person) is established* **organization Name (OID 2.5.4.10):** *organizationName contains full registered name of the subject (legal person).* **organizationIdentifier (2.5.4.97)** (ETSI 319 412 part 1 and 3):

	organizationIdentifier contains an identification of the subject organization different from the organization name VAT or NTR || Code country || - || identifier **commonName (OID 2.5.4.3):** *commonName contains name commonly used by the subject to represent itself. This name needs not be an exact match of the fully registered organization name* **givenName (OID 2.5.4.42)**: Optional *EXTENDED NAME OF THE LEGAL REPRESENTATIVE* **Surname (OID 2.5.4.4)**: Optional *EXTENDED SURNAME OF THE LEGAL REPRESENTATIVE* **Dn_Qualifier (OID: 2.5.4.46):** Optional *Dn_Qualifier contains an unique identification code assigned to the Subject by the CA*
SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Extentions	
Authority Information Access Regulation (EU) N 910/2014 Annex I (clause h) RFC 5280	Not critical Acces Method: id-ad-calssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: (depending on Qualified Certificate CA, see below) - 210d6cb17c110b9b: https://docs.namirialtsp.com/documents/NamQES4K.crt - 6ee82fb2ff762f06: https://docs.namirialtsp.com/documents/NamQES.crt - 4158c13a49d29819: https://docs.firmacerta.it/documents/NamirialCAFirmaQualificata.crt - 396162d9e50483a3: https://docs.namirialtsp.com/documents/NamCA4K.crt Access Method: On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.namirialtsp.com/ocsp/certstatus
Authority Key Identifier	Not critical, SHA-1 160 bit of Issuer public key
Subject Key Identifier	Not critical, SHA-1 160 bit of Subject public key

Qualified Certificate Statements (ETSI 319 412-5)	Not critical qcStatements-1 QcCompliance (0.4.0.1862.1.1) - MANDATORY qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" - MANDATORY qcStatements-4 QcSSCD (0.4.0.1862.1.4) - MANDATORY qcStatements-2 QcEuLimitValue (OID: 0.4.0.1862.1.2) - OPTIONAL • it is present if negotiation limits are applicable qcStatements-5 QcEuPDS (0.4.0.1862.1.5) – MANDATORY • EN (ISO 639-1 code) https://docs.namirialtsp.com/documents/PDS/PDS_en.pdf • IT (ISO 639-1 code) https://docs.namirialtsp.com/documents/PDS/PDS_it.pdf qcStatements-6 QcType (0.4.0.1862.1.6) • id-etsi-qct-eseal (0.4.0.1862.1.6.2)
Certificate Policies	Not critical • QCP-l-qcsd (0.4.0.194112.1.3) • Policy OID 1.3.6.1.4.1.36203.1.2.3 Cp: URL: https://docs.namirialtsp.com/ • NCP+ (0.4.0.2042.1.2)
crlDistributionPoint	Not critical Qualifies Certificate CA crlDistributionPoint
KeyUsage	Critical Not Repudiation

Table 7 - QCP-L-QSCD policy for EU qualified certificate issued to a legal person where the private key related to the certificated public key reside in a QSCD

QCP-l Policy for EU qualified certificate issued to a legal person

Version	Version 3
Serial Number	Serial number of the certificates
Signature Algorithm	Sha256, RSA
Issuer	CA Dname
Validity Period	Max 6 Years
Subject (ETSI 319 412-3) (ETSI 319 412-1)	**countryName (OID 2.5.4.6):** *countryName contains the ISO 3166 country code in which the subject (legal person) is established* **organization Name (OID 2.5.4.10):** *organizationName contains full registered name of the subject (legal person).*

	organizationIdentifier (2.5.4.97) (ETSI 319 412 part 1 and 3): *organizationIdentifier contains an identification of the subject organization different from the organization name VAT or NTR || Code country || - || identifier* **commonName (OID 2.5.4.3):** *commonName contains name commonly used by the subject to represent itself. This name needs not be an exact match of the fully registered organization name* **givenName (OID 2.5.4.42)**: Optional *EXTENDED NAME OF THE LEGAL REPRESENTATIVE* **Surname (OID 2.5.4.4)**: Optional *EXTENDED SURNAME OF THE LEGAL REPRESENTATIVE* **Dn_Qualifier (OID: 2.5.4.46):** Optional *Dn_Qualifier contains an unique identification code assigned to the Subject by the CA*
SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Extentions	
Authority Information Access Regulation (EU) N 910/2014 Annex I (clause h) RFC 5280	Not critical Acces Method: id-ad-calssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: (depending on Qualified Certificate CA, see below) - 210d6cb17c110b9b: https://docs.namirialtsp.com/documents/NamQES4K.crt - 6ee82fb2ff762f06: https://docs.namirialtsp.com/documents/NamQES.crt -4158c13a49d29819: https://docs.firmacerta.it/documents/NamirialCAFirmaQualificata.crt - 396162d9e50483a3: https://docs.namirialtsp.com/documents/NamCA4K.crt Access Method: On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.namirialtsp.com/ocsp/certstatus
Authority Key Identifier	Not critical, SHA-1 160 bit of Issuer public key
Subject Key Identifier	Not critical, SHA-1 160 bit of Subject public key

Qualified Certificate Statements (ETSI 319 412-5)	Not critical qcStatements-1 QcCompliance (0.4.0.1862.1.1) - MANDATORY qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" - MANDATORY qcStatements-2 QcEuLimitValue (OID: 0.4.0.1862.1.2) - OPTIONAL • it is present if negotiation limits are applicable qcStatements-5 QcEuPDS (0.4.0.1862.1.5) – MANDATORY • EN (ISO 639-1 code) https://docs.namirialtsp.com/documents/PDS/PDS_en.pdf • IT (ISO 639-1 code) https://docs.namirialtsp.com/documents/PDS/PDS_it.pdf qcStatements-6 QcType (0.4.0.1862.1.6) • id-etsi-qct-eseal (0.4.0.1862.1.6.2)
Certificate Policies	Not critical • QCP-l (0.4.0.194112.1.1) • Policy OID 1.3.6.1.4.1.36203.1.2.1 Cp: URL: https://docs.namirialtsp.com/ • NCP (0.4.0.2042.1.1)
crlDistributionPoint	Not critical Qualifies Certificate CA crlDistributionPoint
KeyUsage	Critical Not Repudiation

Table 8 - QCP-L policy for EU qualified certificate issued to a legal person

QCP-n-qscd Policy for EU qualified certificate issued to a natural person where the private key related to the certificated public key resides in a QSCD (smart card or hsm)

Version	Version 3
Serial Number	Serial number of the certificates
Signature Algorithm	Sha256, RSA
Issuer	CA Dname
Validity Period	Max 6 Years
Subject (ETSI 319 412-3) (ETSI 319 412-2) (ETSI 319 412-1)	**countryName (OID 2.5.4.6):** *countryName contains the ISO 3166 country code in which the subject resides or in which the entity specified in organizationName (if present) is established.* **organization Name (OID 2.5.4.10):** **OPTIONAL**

	organizationName contains full registered name of the organization associated with the subject. **organizationIdentifier (2.5.4.97)** (ETSI 319 412 part 1,2 and 3): **OPTIONAL** *organizationIdentifier contains an identification of the organization identified in organizationName attribute.* *VAT or NTR || Code country || - || identifier* **commonName (OID 2.5.4.3):** *commonName contains a name of the subject. This may be in the subject's preferred presentation format, or a format preferred by the CA, or some other format. Pseudonyms, nicknames, and names with spelling other than defined by the registered name may be used* **givenName (OID 2.5.4.42) and Surname (OID 2.5.4.4)**: **as an alternative respect to pseudonym:** First name and Last name of the subject **pseudonym (OID 2.5.4.65)** **as an alternative respect to GivenName and SurName:** *pseudonym contains a unique string suitable to identify the subject within CA environment and which can't be used to retrieve Subject's Identity* **serialnumber (OID 2.5.4.65):** *serialNumber contains Tax Indentification Number of the Subject.* *In the eventa that this information isn't available it's possible to use identification document serial number.* *If it's not possible to use id document's serial number it's possible to use other identification numbers assigned by a government o civil authority. In such a case it's possible to use a code derived by one of the previous ones.* **Dn_Qualifier (OID: 2.5.4.5):** Optional

	Dn_Qualifier contains an unique identification code assigned to the Subject by the CA **Title (OID: 2.5.4.12):** Optional *Title contains a value further qualifying the Subject.*
SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Extentions	
Authority Information Access Regulation (EU) N 910/2014 Annex I (clause h) RFC 5280	Not critical Acces Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: (depending on Qualified Certificate CA, see below) - 210d6cb17c110b9b: https://docs.namirialtsp.com/documents/NamQES4K.crt - 6ee82fb2ff762f06: https://docs.namirialtsp.com/documents/NamQES.crt -4158c13a49d29819: https://docs.namirialtsp.com/documents/NamirialCAFirmaQualificata.crt - 396162d9e50483a3: https://docs.namirialtsp.com/documents/NamCA4K.crt Access Method: On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.namirialtsp.com/ocsp/certstatus
Authority Key Identifier	Not critical, SHA-1 160 bit of Issuer public key
Subject Key Identifier	Not critical, SHA-1 160 bit of Subject public key
Qualified Certificate Statements (ETSI 319 412-5)	Not critical qcStatements-1 QcCompliance (0.4.0.1862.1.1) - MANDATORY qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" - MANDATORY qcStatements-4 QcSSCD (0.4.0.1862.1.4) - MANDATORY qcStatements-2 QcEuLimitValue (OID: 0.4.0.1862.1.2) - OPTIONAL • it is present if negotiation limits are applicable qcStatements-5 QcEuPDS (0.4.0.1862.1.5) – MANDATORY • EN (ISO 639-1 code) https://docs.namirialtsp.com/documents/PDS/PDS_en.pdf • IT (ISO 639-1 code) https://docs.namirialtsp.com/documents/PDS/PDS_it.pdf qcStatements-6 QcType (0.4.0.1862.1.6) • id-etsi-qct-esign (0.4.0.1862.1.6.1)
Certificate Policies	Not critical • QCP-n-qcsd (0.4.0.194112.1.2) • Policy OID 1.3.6.1.4.1.36203.1.1.2 (smart card)

	Cp: URL: https://docs.namirialtsp.com/ • NCP+ (0.4.0.2042.1.2) Or • QCP-n-qcsd (0.4.0.194112.1.2) • Policy OID 1.3.6.1.4.1.36203.1.1.5 (HSM) Cp: URL: https://docs.namirialtsp.com/ • NCP+ (0.4.0.2042.1.2)
crlDistributionPoint	Not critical Qualifies Certificate CA crlDistributionPoint
KeyUsage	Critical Not Repudiation

Table 9 - QCP-N-QSCD policy for EU qualified certificate issued to a natural person where the private key related to the certificated public key reside in a QSCD (smart card or HSM)

QCP-n-qscd Policy for EU qualified certificate issued to a natural person where the private key related to the certificated public key resides in a QSCD (smart card or hsm) with etsi en 319 412-2 type 'B' or TYPE 'D' OR type 'f' key usage

Version	Version 3
Serial Number	Serial number of the certificates
Signature Algorithm	Sha256, RSA
Issuer	CA Dname
Validity Period	Max 6 Years
Subject (ETSI 319 412-3) (ETSI 319 412-2) (ETSI 319 412-1)	**countryName (OID 2.5.4.6):** *countryName contains the ISO 3166 country code in which the subject resides or in which the entity specified in organizationName (if present) is established.* **organization Name (OID 2.5.4.10):** **OPTIONAL** *organizationName contains full registered name of the organization associated with the subject.* **organizationIdentifier (2.5.4.97)** (ETSI 319 412 part 1,2 and 3): **OPTIONAL**

	organizationIdentifier contains an identification of the organization identified in organizationName attribute. *VAT or NTR || Code country || - || identifier* **commonName (OID 2.5.4.3):** *commonName contains a name of the subject. This may be in the subject's preferred presentation format, or a format preferred by the CA, or some other format. Pseudonyms, nicknames, and names with spelling other than defined by the registered name may be used* **givenName (OID 2.5.4.42) and Surname (OID 2.5.4.4)**: **as an alternative respect to pseudonym:** First name and Last name of the subject **pseudonym (OID 2.5.4.65)** **as an alternative respect to GivenName and SurName:** *pseudonym contains a unique string suitable to identify the subject within CA environment and which can't be used to retrieve Subject's Identity* **serialnumber (OID 2.5.4.65):** *serialNumber contains Tax Indentification Number of the Subject.* *In the eventa that this information isn't available it's possible to use identification document serial number.* *If it's not possible to use id document's serial number it's possible to use other identification numbers assigned by a government o civil authority. In such a case it's possible to use a code derived by one of the previous ones.* **Dn_Qualifier (OID: 2.5.4.5):** Optional *Dn_Qualifier contains an unique identification code assigned to the Subject by the CA* **Title (OID: 2.5.4.12):** Optional *Title contains a value further qualifying the Subject.*

SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Extentions	
Authority Information Access Regulation (EU) N 910/2014 Annex I (clause h) RFC 5280	Not critical Acces Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: (depending on Qualified Certificate CA, see below) - 210d6cb17c110b9b: https://docs.namirialtsp.com/documents/NamQES4K.crt - 6ee82fb2ff762f06: https://docs.namirialtsp.com/documents/NamQES.crt - 4158c13a49d29819: https://docs.namirialtsp.com/documents/NamirialCAFirmaQualificata.crt - 396162d9e50483a3: https://docs.namirialtsp.com/documents/NamCA4K.crt Access Method: On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.namirialtsp.com/ocsp/certstatus
Authority Key Identifier	Not critical, SHA-1 160 bit of Issuer public key
Subject Key Identifier	Not critical, SHA-1 160 bit of Subject public key
Qualified Certificate Statements (ETSI 319 412-5)	Not critical qcStatements-1 QcCompliance (0.4.0.1862.1.1) - MANDATORY qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" - MANDATORY qcStatements-4 QcSSCD (0.4.0.1862.1.4) - MANDATORY qcStatements-2 QcEuLimitValue (OID: 0.4.0.1862.1.2) - OPTIONAL • it is present if negotiation limits are applicable qcStatements-5 QcEuPDS (0.4.0.1862.1.5) – MANDATORY • EN (ISO 639-1 code) https://docs.namirialtsp.com/documents/PDS/PDS_en.pdf • IT (ISO 639-1 code) https://docs.namirialtsp.com/documents/PDS/PDS_it.pdf qcStatements-6 QcType (0.4.0.1862.1.6) • id-etsi-qct-esign (0.4.0.1862.1.6.1)
Certificate Policies	Not critical • QCP-n-qcsd (0.4.0.194112.1.2) • Policy OID 1.3.6.1.4.1.36203.1.1.2 (smart card) Cp: URL: https://docs.namirialtsp.com/ • NCP+ (0.4.0.2042.1.2) Or • QCP-n-qcsd (0.4.0.194112.1.2) • Policy OID 1.3.6.1.4.1.36203.1.1.5 (HSM)

	Cp: URL: https://docs.namirialtsp.com/ • NCP+ (0.4.0.2042.1.2) All the Qualifed Certificates issued under this profile bring the following limitation of usage: *"L'utilizzo del Certificato è limitato ai rapporti con organismi del settore pubblico / The use of the certificate is limited to relations with public sector bodies"*
crlDistributionPoint	Not critical Qualifies Certificate CA crlDistributionPoint
KeyUsage	Critical One value among ETSI EN 319 412-2 TYPE B or TYPE D or TYPE F values

Table 10 - QCP-N-QSCD policy for EU qualified certificate issued to a natural person where the private key related to the certificated public key resides in a QSCD (smart card or HSM) with ETSI EN 319 412-2 TYPE 'B' or TYPE 'D' or TYPE 'F' KEY USAGE

QCP-n-qscd-A - Policy for EU qualified certificate issued to a natural person (retail) where the private key related to the certificated public key resides in a QSCD for automatic signature

Version	Version 3
Serial Number	Serial number of the certificates
Signature Algorithm	Sha256, RSA
Issuer	CA Dname
Validity Period	Max 6 Years
Subject (ETSI 319 412-3) (ETSI 319 412-2) (ETSI 319 412-1)	**countryName (OID 2.5.4.6):** *countryName contains the ISO 3166 country code in which the subject resides or in which the entity specified in organizationName (if present) is established.* **organization Name (OID 2.5.4.10):** **OPTIONAL** *organizationName contains full registered name of the organization associated with the subject.* **organizationIdentifier (2.5.4.97)** (ETSI 319 412 part 1,2 and 3): **OPTIONAL**

	organizationIdentifier contains an identification of the organization identified in organizationName attribute. *VAT or NTR || Code country || - || identifier* **commonName (OID 2.5.4.3):** *commonName contains a name of the subject. This may be in the subject's preferred presentation format, or a format preferred by the CA, or some other format. Pseudonyms, nicknames, and names with spelling other than defined by the registered name may be used* **givenName (OID 2.5.4.42) and Surname (OID 2.5.4.4)**: **as an alternative respect to pseudonym:** First name and Last name of the subject **pseudonym (OID 2.5.4.65)** **as an alternative respect to GivenName and SurName:** *pseudonym contains a unique string suitable to identify the subject within CA environment and which can't be used to retrieve Subject's Identity* **serialnumber (OID 2.5.4.65):** *serialNumber contains Tax Indentification Number of the Subject.* *In the eventa that this information isn't available it's possible to use identification document serial number.* *If it's not possible to use id document's serial number it's possible to use other identification numbers assigned by a government o civil authority. In such a case it's possible to use a code derived by one of the previous ones.* **Dn_Qualifier (OID: 2.5.4.5):** Optional *Dn_Qualifier contains an unique identification code assigned to the Subject by the CA* **Title (OID: 2.5.4.12):** Optional *Title contains a value further qualifying the Subject.*

SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Extentions	
Authority Information Access Regulation (EU) N 910/2014 Annex I (clause h) RFC 5280	Not critical Acces Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: (depending on Qualified Certificate CA, see below) - 210d6cb17c110b9b: https://docs.namirialtsp.com/documents/NamQES4K.crt - 6ee82fb2ff762f06: https://docs.namirialtsp.com/documents/NamQES.crt - 4158c13a49d29819: https://docs.namirialtsp.com/documents/NamirialCAFirmaQualificata.crt - 396162d9e50483a3: https://docs.namirialtsp.com/documents/NamCA4K.crt Access Method: On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.namirialtsp.com/ocsp/certstatus
Authority Key Identifier	Not critical, SHA-1 160 bit
Subject Key Identifier	Not critical, SHA-1 160 bit
Qualified Certificate Statements (ETSI 319 412-5)	Not critical qcStatements-1 QcCompliance (0.4.0.1862.1.1) - MANDATORY qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" - MANDATORY qcStatements-4 QcSSCD (0.4.0.1862.1.4) - MANDATORY qcStatements-2 QcEuLimitValue (OID: 0.4.0.1862.1.2) - OPTIONAL • it is present if negotiation limits are applicable qcStatements-5 QcEuPDS (0.4.0.1862.1.5) – MANDATORY • EN (ISO 639-1 code) https://docs.namirialtsp.com/documents/PDS/PDS_en.pdf • IT (ISO 639-1 code) https://docs.namirialtsp.com/documents/PDS/PDS_it.pdf qcStatements-6 QcType (0.4.0.1862.1.6) • id-etsi-qct-esign (0.4.0.1862.1.6.1)
Certificate Policies	Not critical • QCP-n-qcsd (0.4.0.194112.1.2) • Policy OID 1.3.6.1.4.1.36203.1.1.3 (HSM Automatica) Cp: URL: https://docs.namirialtsp.com/ • NCP+ (0.4.0.2042.1.2)
crlDistributionPoint	Not critical Qualifies Certificate CA crlDistributionPoint
KeyUsage	Critical Not Repudiation

Table 11 - QCP-N-QSCD-A - policy for EU qualified certificate issued to a natural person (retail) where the private key related to the certificated public key reside in a QSCD for automatic signature

QCP-n-qscd-D - Policy for EU qualified certificate issued to a natural person (retail) where the private key related to the certificated public key resides in a QSCD for disposable signature

Version	Version 3
Serial Number	Serial number of the certificates
Signature Algorithm	Sha256, RSA
Issuer	CA Dname
Validity Period	Max 30 days
Subject (ETSI 319 412-3) (ETSI 319 412-2) (ETSI 319 412-1)	**countryName (OID 2.5.4.6):** *countryName contains the ISO 3166 country code in which the subject resides or in which the entity specified in organizationName (if present) is established.* **organization Name (OID 2.5.4.10):** **OPTIONAL** *organizationName contains full registered name of the organization associated with the subject.* **organizationIdentifier (2.5.4.97)** (ETSI 319 412 part 1,2 and 3): **OPTIONAL** *organizationIdentifier contains an identification of the organization identified in organizationName attribute.* *VAT or NTR || Code country || - || identifier* **commonName (OID 2.5.4.3):** *commonName contains a name of the subject. This may be in the subject's preferred presentation format, or a format preferred by the CA, or some other format. Pseudonyms, nicknames, and names with spelling other than defined by the registered name may be used* **givenName (OID 2.5.4.42) and Surname (OID 2.5.4.4)**: **as an alternative respect to pseudonym:** First name and Last name of the subject

	pseudonym (OID 2.5.4.65) **as an alternative respect to GivenName and SurName:** *pseudonym contains a unique string suitable to identify the subject within CA environment and which can't be used to retrieve Subject's Identity* **serialnumber (OID 2.5.4.65):** *serialNumber contains Tax Indentification Number of the Subject.* *In the eventa that this information isn't available it's possible to use identification document serial number.* *If it's not possible to use id document's serial number it's possible to use other identification numbers assigned by a government o civil authority. In such a case it's possible to use a code derived by one of the previous ones.* **Dn_Qualifier (OID: 2.5.4.5):** Optional *Dn_Qualifier contains an unique identification code assigned to the Subject by the CA* **Title (OID: 2.5.4.12):** Optional *Title contains a value further qualifying the Subject.*
SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Extentions	
Authority Information Access Regulation (EU) N 910/2014 Annex I (clause h) RFC 5280	Not critical Acces Method: id-ad-calssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: (depending on Qualified Certificate CA, see below) - 210d6cb17c110b9b: https://docs.namirialtsp.com/documents/NamQES4K.crt - 6ee82fb2ff762f06: https://docs.namirialtsp.com/documents/NamQES.crt - 4158c13a49d29819: https://docs.namirialtsp.com/documents/NamirialCAFirmaQualificata.crt - 396162d9e50483a3: https://docs.namirialtsp.com/documents/NamCA4K.crt Access Method: On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.namirialtsp.com/ocsp/certstatus

Authority Key Identifier	Not critical, SHA-1 160 bit
Subject Key Identifier	Not critical, SHA-1 160 bit
Qualified Certificate Statements (ETSI 319 412-5)	Not critical qcStatements-1 QcCompliance (0.4.0.1862.1.1) - MANDATORY qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" - MANDATORY qcStatements-4 QcSSCD (0.4.0.1862.1.4) - MANDATORY qcStatements-2 QcEuLimitValue (OID: 0.4.0.1862.1.2) - OPTIONAL • it is present if negotiation limits are applicable qcStatements-5 QcEuPDS (0.4.0.1862.1.5) – MANDATORY • EN (ISO 639-1 code) https://docs.namirialtsp.com/documents/PDS/PDS_en.pdf • IT (ISO 639-1 code) https://docs.namirialtsp.com/documents/PDS/PDS_it.pdf qcStatements-6 QcType (0.4.0.1862.1.6.1) • id-etsi-qct-esign (0.4.0.1862.1.6.1)
Certificate Policies	Not critical • QCP-n-qcsd (0.4.0.194112.1.2) • Policy OID 1.3.6.1.4.1.36203.1.1.6 (HSM Disposable) Cp: URL: https://docs.namirialtsp.com/ • NCP+ (0.4.0.2042.1.2)
crlDistributionPoint	Not critical Qualifies Certificate CA crlDistributionPoint
KeyUsage	Critical Not Repudiation

Table 12 - QCP-N-QSCD-D - policy for EU qualified certificate issued to a natural person (retail) where the private key related to the certificated public key reside in a QSCD for disposable signature

QCP-n-qscd-LD - Policy for EU qualified certificate issued to a natural person (retail) where the private key related to the certificated public key resides in a QSCD for Long-Lived disposable signature

Version	Version 3
Serial Number	Serial number of the certificates
Signature Algorithm	Sha256, RSA
Issuer	CA Dname
Validity Period	30 days

Subject (ETSI 319 412-3) (ETSI 319 412-2) (ETSI 319 412-1)	**countryName (OID 2.5.4.6):** *countryName contains the ISO 3166 country code in which the subject resides or in which the entity specified in organizationName (if present) is established.* **organization Name (OID 2.5.4.10):** **OPTIONAL** *organizationName contains full registered name of the organization associated with the subject.* **organizationIdentifier (2.5.4.97)** (ETSI 319 412 part 1,2 and 3): **OPTIONAL** *organizationIdentifier contains an identification of the organization identified in organizationName attribute.* *VAT or NTR || Code country || - || identifier* **commonName (OID 2.5.4.3):** *commonName contains a name of the subject. This may be in the subject's preferred presentation format, or a format preferred by the CA, or some other format. Pseudonyms, nicknames, and names with spelling other than defined by the registered name may be used* **givenName (OID 2.5.4.42) and Surname (OID 2.5.4.4)**: **as an alternative respect to pseudonym:** First name and Last name of the subject **pseudonym (OID 2.5.4.65)** **as an alternative respect to GivenName and SurName:** *pseudonym contains a unique string suitable to identify the subject within CA environment and which can't be used to retrieve Subject's Identity* **serialnumber (OID 2.5.4.65):** *serialNumber contains Tax Indentification Number of the Subject.* *In the eventa that this information isn't available it's possible to use identification document serial number.*

	If it's not possible to use id document's serial number it's possible to use other identification numbers assigned by a government o civil authority. In such a case it's possible to use a code derived by one of the previous ones. **Dn_Qualifier (OID: 2.5.4.5):** Optional *Dn_Qualifier contains an unique identification code assigned to the Subject by the CA* **Title (OID: 2.5.4.12):** Optional *Title contains a value further qualifying the Subject.*
SubjectPublicKeyInfo	RSA (2048 bits) Algorithm: RSA
Extentions	
Authority Information Access Regulation (EU) N 910/2014 Annex I (clause h) RFC 5280	Not critical Acces Method: id-ad-caIssuers (1.3.6.1.5.5.7.48.2) Alternative Name: URL: (depending on Qualified Certificate CA, see below) - 210d6cb17c110b9b: https://docs.namirialtsp.com/documents/NamQES4K.crt - 6ee82fb2ff762f06: https://docs.namirialtsp.com/documents/NamQES.crt - 4158c13a49d29819: https://docs.namirialtsp.com/documents/NamirialCAFirmaQualificata.crt - 396162d9e50483a3: https://docs.namirialtsp.com/documents/NamCA4K.crt Access Method: On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL: http://ocsp.namirialtsp.com/ocsp/certstatus
Authority Key Identifier	Not critical, SHA-1 160 bit
Subject Key Identifier	Not critical, SHA-1 160 bit
Qualified Certificate Statements (ETSI 319 412-5)	Not critical qcStatements-1 QcCompliance (0.4.0.1862.1.1) - MANDATORY qcStatements-3 QcEuRetentionPeriod (0.4.0.1862.1.3): "20" - MANDATORY qcStatements-4 QcSSCD (0.4.0.1862.1.4) - MANDATORY qcStatements-2 QcEuLimitValue (OID: 0.4.0.1862.1.2) - OPTIONAL • it is present if negotiation limits are applicable qcStatements-5 QcEuPDS (0.4.0.1862.1.5) – MANDATORY • EN (ISO 639-1 code)

	https://docs.namirialtsp.com/documents/PDS/PDS_en.pdf • IT (ISO 639-1 code) https://docs.namirialtsp.com/documents/PDS/PDS_it.pdf qcStatements-6 QcType (0.4.0.1862.1.6.1) • id-etsi-qct-esign (0.4.0.1862.1.6.1)
Certificate Policies	Not critical • QCP-n-qcsd (0.4.0.194112.1.2) • Policy OID 1.3.6.1.4.1.36203.1.1.7 (HSM Long-Lived Disposable) Cp: URL: https://docs.namirialtsp.com/ • NCP+ (0.4.0.2042.1.2)
crlDistributionPoint	Not critical Qualifies Certificate CA crlDistributionPoint
KeyUsage	Critical Not Repudiation

Table 13 - QCP-N-QSCD-LD - policy for EU qualified certificate issued to a natural person (retail) where the private key related to the certificated public key reside in a QSCD for long-lived disposable signature

Appendice C: macro e comandi

Istruzioni macro o codici eseguibili presenti all'interno del documento che modifichino gli atti ed i fatti rappresentati nel documento stesso invalidano la firma (art. 4, comma 3 del DPCM. È cura del Titolare assicurarsi, tramite le funzionalità tipiche di ogni prodotto, dell'assenza di tali codici eseguibili.
Di seguito si riportano i passaggi utili a disabilitare le istruzioni macro o codici eseguibili per i prodotti maggiormente diffusi. Per i dettagli si rimanda ai manuali d'uso forniti a corredo delle applicazioni.

MS Word® 2003 e MS Excel® 2003
Per disattivare le macro seguire la seguente procedura:

- selezionare tutto il testo e quindi premere contemporaneamente i tasti Ctrl+Shift+F9.

MS Word® 2007 e MS Excel® 2007
Per disattivare le macro seguire i seguenti passi:

- cliccare sul pulsante Office,
- cliccare su Opzioni,
- cliccare su Centro protezione,
- posizionarsi su Impostazioni Centro protezione,
- cliccare su Disattiva tutte le macro con notifica.

MS Word® 2010/2013 e MS Excel® 2010/2013
Per disattivare le macro seguire i seguenti passi:

- cliccare sul pulsante File,
- cliccare su Opzioni,
- cliccare su Centro protezione,
- posizionarsi su pulsante Impostazioni Centro protezione,
- cliccare su Disattiva tutte le macro con notifica.

Adobe Acrobat®
Per disattivare le funzioni di esecuzione di codice JavaScript seguire i passi:

- cliccare su Modifica,
- cliccare su Preferenze,
- JavaScript,
- rimuovere il flag di abilitazione del JavaScript.