Timestamping Authority Policy and Practice Statement

Sommario

1 Introduzione

Le marche Temporali qualificate è il processo per tenere traccia in modo sicuro dei tempi di creazione e modifica di un documento. Sicurezza qui significa che nessuno - nemmeno il proprietario del documento - dovrebbe essere in grado di cambiarlo una volta che è stato registrato, a condizione che l'integrità del timestamper non sia mai compromessa. A.G.T. Enterprise Srl (di seguito, "AGT") è una società a responsabilità limitata, identificata con numero di partita IVA 02911180608 e sede legale in Corso della Repubblica 184 Cassino FR ITALY. AGT è un fornitore di servizi di firma elettronica avanzata e remota e intende descrivere le regole e le procedure operative che verranno adottate per la fornitura di marca temporale qualificate ai sensi del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 e in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche in accordo ai requisiti descritti nella normativa ETSI EN 319 421.

1.1 Scopo

Lo scopo di questo documento e di fornire le policy e gli aspetti operativi di AGT TSA. Il TSA sarà identificato con l'identità degli oggetti (OID) di AGT Enterprise fornito dall' I.A.N.A: 1.3.6.1.4.1.56434.1.10.1 La sua ultima versione è sempre disponibile al seguente link:

http://ca.agtenterprise.it/AGT Enterprise _CPS_CA.pdf

Questo documento è modificato e aggiornato secondo la Sezione 1.5 del CPS.

2 Riferimenti

- Recommendation ITU-R TF.460-6 (2002): "Standard-frequency and time-signal emissions".
- ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers"
- ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps"
- ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles"
- 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 319 122 - CAdES digital signatures
- IETF (RFC3161) https://www.ietf.org/rfc/rfc3161.txt
- IETF (RFC3628) https://www.ietf.org/rfc/rfc3628.txt

2.1 Technical Standards

- ETSI EN 319 401 – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- ETSI EN 319 421 - Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- ETSI EN 319 422 - Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

3 Acronyms and Synonyms

- **Certification Authority (CA):** Un sistema fiduciario gestito da un Trust Service Provider e responsabile dell'emissione e della revoca dei certificati utilizzati nelle firme elettroniche. Da un punto di vista giuridico si tratta di un caso specifico di Trust Service Provider e, per estensione, il provider è denominato Certification Authority.
- **Certification Practice Statement (CPS):** È un documento di un'Autorità di certificazione che descrive la loro pratica per l'emissione e la gestione dei certificati a chiave pubblica

- **Coordinate Universal Time (UTC):** è lo standard orario principale con cui il mondo regola gli orologi e l'ora. È entro circa 1 secondo dall'ora solare media a 0° di longitudine.
- **Information Security Management Policy (ISMS):** Un ISMS, o sistema di gestione della sicurezza delle informazioni, è un sistema di gestione definito e documentato che consiste in un insieme di politiche, processi e sistemi per gestire i rischi per i dati organizzativi, con l'obiettivo di garantire livelli accettabili di rischio per la sicurezza delle informazioni
- **Relying Party**: destinatario di una marca temporale che si basa su tale marca temporale
- **Subscriber**: persona fisica o giuridica a cui è rilasciata la marca temporale e che è tenuta agli obblighi di sottoscrizione.
- **Terms and Conditions**: insieme di dichiarazioni sulle politiche e le pratiche di un TSA che richiedono in particolare enfasi o divulgazione agli abbonati e alle parti di affidamento
- **Time-stamp**: dati in formato elettronico che legano altri dati elettronici a un determinato momento, stabilendo la prova che tali dati esistevano in quel momento
- **Time-Stamping Authority** (TSA): Un TSP che emette marche temporali utilizzando uno o più TSU.
- **Time-Stamp Unit** (TSU): Un insieme di hardware e software gestito come un'unità e che dispone sempre di un'unica chiave di firma attiva.
- **Qualified Trust Service Provider** (TSP): soggetto che fornisce uno o più servizi fiduciari qualificati. È l'ente preposto alla gestione della CA.

4 General Concepts

4.1 Timestamping services

- Time-stamping provision: Questo componente del servizio genera marche temporali qualificati.

- **Time-stamping management**: Questo componente del servizio monitora e controlla il funzionamento dei servizi di marcatura temporale per garantire che il servizio fornito sia conforme a quanto specificato dalla TSA. Questo componente del servizio è responsabile dell'installazione e della disinstallazione del servizio di fornitura di marca temporale.

4.1.1 Uso di marche temporali qualificate

- Per preservare l'integrità di un documento dopo che è stata utilizzata la firma elettronica avanzata (IOFIRMO) di AGT
- Le marche temporali qualificati possono essere utilizzate solo in conformità a quanto descritto in questo documento.

4.2 Timestamping Authority

La TSA di AGT è responsabile del funzionamento di uno o più servizi di marca temporale identificati nella precedente sezione 4.1 ed esempi sono stati forniti nella sezione 4.1.1.
La AGT-TSA ha la responsabilità del funzionamento di una o più TSU che crea e firma per conto della AGT-TSA. Inoltre, la AGT-TSA è responsabile di garantire che i requisiti identificati nella presente Dichiarazione di politica e pratica siano soddisfatti.

4.3 Utenti

Un firmatario è l'utente finale delle marche temporali qualificati emessi da uno dei TSU gestisti dalla AGT-TSA. I firmatari possono essere persone fisiche o enti (pubblici o privati), nonché apparecchiature tecnologiche.

4.4 Relying Party

Un individuo o un'organizzazione (pubblica o privata), destinatario di una marca temporale qualificata che fa affidamento su tale marca temporale qualificata.

4.5 Time-stamp policy and TSA practice statement

Questo documento deve essere letto insieme alla versione del Certification Policy Statement (TSP-CPS) pubblicato sul sito di AGT Enterprise, disponibile al seguente link:

http://ca.agtenterprise.it/AGT Enterprise _CPS_CA.pdf

Questo documento specifica la policy e l'operatività per il servizio di marca temporale qualificato fornito da AGT, che insieme al TSP-CPS e ad altri documenti interni è conforme alla legislazione e agli standard tecnici.

Tale policy, infine, illustra a livello generale, senza descrivere alcun dettaglio tecnico circa il sistema informativo e le comunicazioni, la struttura organizzativa e le modalità operative e di protezione. Questa policy non definisce l'ambiente di elaborazione in cui è in esecuzione il servizio; queste questioni sono definite nel TSP-CPS di AGT Enterprise.

5 Time-stamp Policies and General Requirements

5.1 General

Per **Time-Stamp Policy** si definisce un insieme di processi per la creazione di marcature temporali qualificate, secondo gli standard tecnici. La AGT-TSA firma elettronicamente marcature temporali qualificate utilizzando chiavi private appositamente riservate a questo scopo. Le chiavi private di firma delle marche temporali qualificati sono archiviate in un dispositivo crittografico (HSM) dedicato e approvato. Ogni marca temporale qualificato contiene un identificatore di criterio e viene emesso con una precisione di 1 secondo o più. Le marche temporali qualificati vengono ordinati tramite il Transmission Control Protocol (TCP) o l'Hypertext Transfer Protocol (HTTP), come specificato negli standard tecnici.

5.2 Identification

OID di identificazione dell'oggetto Timestamp è: 1.3.6.1.4.1.56434.1.10.1 Questo identificatore è referenziato in tutte le marche temporali qualificate emesse da Time Stamp Authority di AGT e questa politica è disponibile per tutti gli abbonati e le parti a cui affidare.

5.3 User community and applicability

La comunità di utenti per i servizi di marche temporali qualificati di AGT-TSA comprende i suoi firmatari che utilizzano il servizio di IOFIRMO.

5.4 Compliance

AGT-TSA è soggetta ad audit esterni e interni indipendenti, al fine di dimostrare che il servizio di marca temporale qualificato adempie agli obblighi stabiliti dalla Legislazione Applicabile e ha implementato controlli appropriati come descritto nella Sezione 7.

5.5 Time-stamp format

I token di marca temporale emessi da AGT-TSA sono conformi a RFC 3161 [7] marcature temporali. Il servizio emette timestamp crittografati RSA2048 che accettano l'algoritmo hash SHA256.

5.6 Time accuracy

Il servizio di timestamp utilizza questo segnale orario e un insieme di server ntp come origini dell'ora. Con tale impostazione il servizio di marcatura temporale raggiunge una precisione del tempo di +/- 1s o migliore rispetto all'UTC.

Limitazioni del Servizio

La QTSP AGT Enterprise ha stipulato un contratto di assicurazione a copertura dei rischi dell'attività e dei danni causati a terzi, il cui testo è stato inviato all'ente italiano AgID.

Obblighi dell'abbonato

Si prega di consultare "Termini e condizioni per il cliente di marca temporale" per informazioni dettagliate.

Obblighi dell'affidatario

Si prega di consultare "Termini e condizioni per il cliente di marca temporale" per informazioni dettagliate.

Verifica della marca temporale

La verifica delle marche temporali include i seguenti passaggi:

Passaggio I: verifica dello stato di revoca delle marche temporali

La verifica del periodo di validità del certificato TSU e della validità della chiave di firma viene verificata utilizzando lo stato di revoca corrente per il certificato TSU tramite ocsp, disponibile su http://ca.agtenterprise.it/tsa_cert-ocsp.

Passaggio II: verifica dell'integrità delle marche temporali

L'integrità crittografica della marche temporali, ad esempio la corretta struttura ASN.1, e il dato di appartenenza possono essere verificati con il client "IOFIRMO"

5.7 Term and conditions

Una marcha temporale qualificata è un certificato elettronico che indica l'esistenza di determinati dati. AGT Enterprise (TSP) è un prestatore di servizi fiduciari qualificato secondo le regole del regolamento eIDAS.

L'esecuzione di marcature temporali qualificate e firme temporali viene fornita via Internet solo nell'ambito di contratti di servizio e/o di licenza legati al servizio di IOFRIMO.

AGT Enterprise garantisce la disponibilità del servizio di marca temporale solo agli utenti sottoscrittori di IOFIRMO salvo il caso di attività di manutenzione programmata, preventivamente comunicata agli utenti du IOFIRMO. AGT Enterprise TSP ha la facoltà in qualsiasi momento di effettuare manutenzioni, upgrade o modifiche senza che tali perdite vengano prese in considerazione nel calcolo della disponibilità dei principali servizi.

AGT Enterprise TSP informerà il cliente prima della data prevista dell'interruzione dei servizi chiave quali manutenzioni, aggiornamenti o modifiche, almeno quattordici giorni.

I protocolli di marca temporale, ovvero ogni marca temporale emessa, vengono conservati per almeno 20 anni.

5.8 Information security policy

AGT Enterprise ha implementato una politica di sicurezza delle informazioni in tutta l'azienda in accordo con la normativa ISO 270001. Tutti i dipendenti devono attenersi alle norme stabilite in tale politica e ai concetti di sicurezza derivati. La politica di sicurezza delle informazioni viene rivista regolarmente e quando si verificano cambiamenti significativi. L'Alta Direzione di AGT Enterprise approva le modifiche alla politica di sicurezza delle informazioni.

5.9 TSA obligations

Il rispetto delle procedure indicate nel presente documento è assicurato da AGT Enterprise. Un organismo di vigilanza indipendente verifica periodicamente l'efficacia delle procedure.

5.9.1 TSA obligations towards subscribers

Il presente documento non pone obblighi specifici all'abbonato oltre a eventuali requisiti specifici della TSA indicati nella clausola 6.3, Termini e condizioni.

5.6 Information for relying parties

Gli obblighi dell'utente valgono anche per gli affidatari. Inoltre, la parte ricorrente deve:

- verificare che la marca temporale sia stata correttamente firmata e che la chiave privata utilizzata per firmare la marca temporale non sia stata compromessa fino al momento della verifica;
- tenere conto di eventuali limitazioni all'uso della marca temporale indicate dalla politica di marca temporale;
- tenere conto di ogni altra precauzione prescritta in accordi o altrove.

6 Obligations and Liability

6.1 TSA's obligations and liabilities

AGT Enterprise gestisce la TSA e si assume la responsabilità dei requisiti descritti nella sezione 7 di questo documento, nonché la conformità agli standard tecnici e alla legislazione applicabile. Tali doveri e responsabilità sono regolati da accordi reciproci sottoscritti tra le parti, di cui sono parti integranti la Policy and Practice Statement

dell'Autorità per la Marcatura temporale e il CPS. Inoltre, AGT Enterprise assume nei confronti dei sottoscrittori del servizio di marca temporale qualificata i seguenti obblighi:

- La sua attività di marca temporale qualificata si basa su apparecchiature e software certificati, conformi alle Norme Tecniche e alla Legislazione Applicabile.
- È conforme alla Policy and Practice Statement della Timestamping Authority e del CPS.
- Assicura che i timestamp qualificati mantengano un'accuratezza di almeno un (1) secondo rispetto all'UTC.
- È sottoposto ad audit e valutazioni interne ed esterne per garantire la conformità agli Standard Tecnici e alla Legislazione Applicabile.

Fornisce un accesso ad alta disponibilità ai sistemi per l'ottenimento di marcature temporali qualificate, salvo nei casi di interruzioni tecniche programmate, perdita di sincronizzazione dell'ora e altri casi descritti nella Sezione 9.8 del CPS.

6.2 Subscriber's obligations

- Gli utenti devono assicurarsi che i timestamp qualificati siano stati firmati correttamente e controllare la CRL per confermare che la chiave privata utilizzata per firmare questi timestamp qualificati non sia compromessa. La CRL può essere verificata al seguente link: http://pki.AGT Enterprise.com/crl

6.3 Relying parties' obligations

- a) Deve assicurarsi che i timestamp qualificati siano stati firmati correttamente e controllare la CRL per confermare che la chiave privata utilizzata per firmare questi timestamp qualificati non sia compromessa. La CRL può essere verificata al seguente link:

  http://ca.agtenterprise.it/tsacrl

6.4 Liability

AGT Enterprise si impegna a gestire il servizio di marca temporale qualificato in conformità con la presente Policy per la marcatura temporale, il CPS, gli standard tecnici e la legislazione applicabile.

6.5 Risk assessment

AGT Enterprise TSP esegue regolarmente valutazione dei rischi per garantire la qualità e l'affidabilità dei servizi di marcatura temporale. I controlli di sicurezza definiti in un concetto di sicurezza dei servizi di marcatura temporale sono controllati regolarmente al fine di garantire l'efficienza dei controlli.

5.2 **Trust Service Practice Statement**

Il presente documento definisce gli elementi generali della politica e della pratica di CSP e fornisce TSS in qualità di condizioni generali. La Politica definisce le condizioni e le regole a cui CSP aderisce.

Inoltre, per essere conformi a ETSI EN 319 401 [2], per ogni marca temporale le seguenti politiche sono supportate da AGT Enterprise TSA:

7 TSA Management and Operation

7.1 TSU Key generation

AGT Enterprise genera le chiavi crittografiche utilizzate per la firma di marca temporale qualificata in un dispositivo HSM, certificato secondo FIPS 140-2 Livello 3, da personale autorizzato, sotto doppio controllo, in un ambiente fisico sicuro. La TSA emette timestamp qualificati firmati con una chiave RSA di 2048 bit di lunghezza, che accetta gli algoritmi hash SHA256, SHA512.

7.2 TSU private key protection

AGT Enterprise ha adottato misure specifiche per garantire che le chiavi private utilizzate per la firma delle marche temporali qualificate rimangano riservate e mantengano la loro integrità. Queste misure includono l'uso di HSM certificati secondo FIPS 140-2 Livello 3. Quando vengono eseguite copie di backup di queste chiavi, questa procedura viene eseguita da personale autorizzato, che richiede almeno una doppia custodia e un ambiente fisico sicuro. In ogni caso, le copie di backup non vengono mai eseguite avendo accesso diretto al materiale della chiave privata, ma viene copiato un blob di chiavi crittografato con la chiave master HSM.

7.3 TSU public key certificate

La TSA garantisce l'integrità e l'autenticità delle chiavi (pubbliche) di verifica della firma della TSU come segue:

- La verifica della firma della TSU (chiavi pubbliche) è disponibile per le parti che si affidano a un certificato a chiave pubblica. Gli attestati sono pubblicati al seguente link:
  a) http://ca.agtenterprise.it/tsacert
- La TSU non rilascia una marca temporale qualificata prima che il suo certificato di verifica della firma (chiave pubblica) sia caricato nella TSU o nel suo dispositivo crittografico.
- Quando si ottiene un certificato di verifica della firma (chiave pubblica), la TSA verifica che questo certificato sia stato firmato correttamente (compresa la verifica della catena di certificati a un'autorità di certificazione attendibile)

7.4 Rekeying TSU's key

La chiave TSU ha una durata valida di 20 anni. Prima che la data di scadenza della chiave sia soddisfatta, una nuova coppia di chiavi e un certificato verranno generati e collocati in posizione per continuare con il servizio

Per ogni operazione di rekeying della TSU, viene eseguita un'analisi per verificare che gli algoritmi crittografici utilizzati dalla TSU siano ancora riconosciuti come idonei. In caso contrario, vengono modificati per conformarsi alle raccomandazioni crittografiche fornite da organizzazioni riconosciute come il NIST.

7.5 End of TSU key life cycle

Le chiavi utilizzate dal servizio di marca temporale qualificato vengono sostituite dopo la sua scadenza. Le marche temporali qualificate non vengono emesse utilizzando le chiavi scadute. Dopo la sua scadenza, le chiavi private vengono distrutte.

7.6 Life cycle management of signing cryptographic hardware

AGT Enterprise ha adottato misure specifiche per garantire che i moduli crittografici (HSM) utilizzati nei servizi di non ripudio non vengano violati durante il trasporto o lo stoccaggio. Tutti gli HSM sono re inizializzato prima dell'uso, da personale autorizzato, sotto doppio controllo e in un ambiente fisico sicuro. Ogni volta che un HSM viene sottoposto a intervento tecnico o disabilitato, tutte le chiavi memorizzate vengono cancellate secondo le istruzioni del produttore.

7.7 Time-stamping

7.7.1 Time-stamp issuance

Le marche temporali qualificate vengono emesse in conformità con il profilo di marca temporale definito in ETSI EN 319 422[5] e sono conformi alla RFC 3161 "Time Stamp Protocol (TSP)". Ciascun TST contiene l'identificatore della politica di marcatura temporale, un numero di serie univoco e un certificato contenente le informazioni di identificazione del TSU di AGT Enterprise TSA se richiesto dal cliente.
La TSU accetta le richieste utilizzando SHA224, SHA256, SHA383 e SHA512 come algoritmo hash per ottenere il digest.
La chiave TSU è una chiave RSA a 2048 bit utilizzata solo per la firma dei TST.
Per ogni richiesta di marca temporale qualificata, la TSA genera record di audit inclusi dati sull'ora della richiesta, risultato della richiesta, marca temporale emessa e dati aggiuntivi per garantire l'integrità dei record di audit.

La TSU non emette alcun TST se è stata raggiunta la fine della validità del certificato TSU o se l'accuratezza temporale del sistema rispetto a un insieme attendibile di server NTP è superiore a un secondo

7.7.2 Clock synchronization with UTC

Il TSA è sincronizzato con UTC [ROA] con una precisione di 1 secondo o migliore utilizzando il protocollo NTP. Il TSA è sincronizzato con diversi server NTP per i quali viene eseguito periodicamente un polling assicurandosi che l'accuratezza temporale sia sempre inferiore al secondo, che è il massimo consentito. Se si verifica un errore e viene rilevata una precisione dell'ora superiore a un secondo, la TSA non emetterà timestamp come indicato in ETSI EN 319 421. AGT Enterprise Il TSA è sincronizzato con UTC [ROA] con una precisione di 1 secondo o migliore utilizzando il protocollo NTP.
TSA assicura che il suo orologio sia sincronizzato con l'UTC entro la precisione dichiarata seguendo i requisiti:

- la calibrazione degli orologi TSU deve essere mantenuta in modo tale che non ci si possa aspettare che gli orologi si spostino al di fuori dell'accuratezza dichiarata;
- la precisione dichiarata è di 1 secondo o migliore;

- gli orologi TSU sono protetti contro i danni che potrebbero comportare una modifica non rilevata dell'orologio che lo porti al di fuori della sua calibrazione;
- la TSA garantisce che, se l'ora che sarebbe indicata in un token di marca temporale si sposta o non si sincronizza con l'UTC, questa venga rilevata;
- vengono registrati i record relativi a tutti gli eventi relativi alla sincronizzazione dell'orologio di una TSU con l'UTC. Ciò include informazioni relative alla normale ricalibrazione o sincronizzazione degli orologi utilizzati nella marcatura temporale;
- vengono registrati i record relativi a tutti gli eventi relativi al rilevamento della perdita di sincronizzazione.

7.8 Physical and environmental security

Si prega di rivedere la Sezione 5.1 del CPS. AGT Enterprise TSP controlla l'accesso fisico ai componenti del proprio sistema PKI, la cui sicurezza è fondamentale per la fornitura dei propri servizi fiduciari e per ridurre al minimo i rischi relativi alla sicurezza fisica. AGT Enterprise TSP garantisce che la posizione e la costruzione della struttura che ospita le apparecchiature TSA siano coerenti con le strutture per ospitare informazioni sensibili e di alto valore.

7.9 Risk assessment and information security policy

AGT Enterprise ha un ISMS, in base al quale esegue varie valutazioni dei rischi e ci sono varie politiche di sicurezza delle informazioni che governano l'azienda. Nell'ambito di questa valutazione del rischio, la TSA fa parte delle aree esaminabili. L'ISMS è gestito dal Comitato per la sicurezza delle informazioni che esamina e si assicura che AGT Enterprise come azienda e i suoi dipendenti aderiscano e rispettino l'ISMS.

7.10 Operation security

AGT Enterprise TSA garantisce che i componenti del sistema TSA siano sicuri e utilizzati correttamente, con il minimo rischio di guasto. In particolare:

- L'integrità dei componenti e delle informazioni del sistema TSA è protetta da virus, software dannoso e non autorizzato.

- Le procedure di segnalazione e risposta agli incidenti sono impiegate in modo tale da ridurre al minimo i danni derivanti da incidenti e malfunzionamenti di sicurezza.
- I supporti utilizzati all'interno dei sistemi affidabili di AGT Enterprise TSA sono gestiti in modo sicuro per proteggere i supporti da danni, furti, accessi non autorizzati e obsolescenza.
- Le procedure sono stabilite e implementate per tutti i ruoli di fiducia e amministrativi che hanno un impatto sulla fornitura di servizi di timestamp.
- Le richieste di capacità sono monitorate continuamente per garantire che AGT Enterprise TSP possa soddisfare le richieste di disponibilità fornite a tutti i clienti. Le proiezioni di capacità future vengono aggiornate regolarmente per garantire che non si verifichi alcuna interruzione del servizio in nessun momento futuro.

Si prega di rivedere la Sezione 5.2 del CPS.

7.11 Network security

AGT TSP protegge la propria rete e il proprio sistema dagli attacchi, in particolare: 1) segmentando i Sistemi di Certificazione in reti o zone in base alla loro relazione funzionale, logica e fisica; 2) separare la piattaforma di test, certificazione e produzione da altri ambienti non interessati alle operazioni live; 3) mantenere e proteggere i sistemi di emissione, i sistemi di gestione dei certificati e i sistemi di supporto alla sicurezza in una zona sicura; 4) configurare ogni controllo del confine di rete (firewall, switch, router, gateway) con regole che supportino solo i servizi, i protocolli, le porte e le comunicazioni che la TSA ha identificato come necessari alle sue operazioni; 5) configurare tutti i sistemi TSU rimuovendo tutti gli account, servizi, protocolli e porte non utilizzati nelle operazioni della TSA; 6) accordare l'accesso solo ai ruoli fidati alla zona ad alta sicurezza

7.12 Incident management

1) monitors start-up and shutdown of the logging functions and the availability of the network services

2) appoints trusted role personnel to follow up on alerts of potentially critical security events

3) Se si verifica un'interruzione non pianificata del servizio TSA, apre un incidente correlato e lo gestisce al fine di identificare, registrarsi nel sistema di Trouble Ticketing, assegnare priorità e diagnosticare l'incidente

4) Escalation - se il personale di supporto ha bisogno di supporto da altre unità organizzative

5) agisce in modo tempestivo e coordinato al fine di rispondere rapidamente agli incidenti e limitare l'impatto delle violazioni della sicurezza

6) nomina personale di ruolo di fiducia per dare seguito alle segnalazioni di eventi di sicurezza potenzialmente critici e garantire che gli incidenti rilevanti siano segnalati in linea con le procedure del TSP

7) segnala ai soggetti competenti in linea con le norme regolamentari applicabili ogni violazione della sicurezza o perdita di integrità che abbia un impatto significativo sul servizio fiduciario prestato e sui dati personali ivi conservati

8) informa l'organismo di vigilanza nazionale AgID entro 24 ore dalla scoperta di una violazione critica della sicurezza via e-mail

9) Le procedure di segnalazione e risposta agli incidenti sono impiegate in modo tale da ridurre al minimo i danni derivanti da incidenti di sicurezza e malfunzionamenti.

7.13 Collection of evidence

AGT registra e mantiene accessibili per un congruo periodo di 20 anni, anche dopo la cessazione delle attività del TSP, tutte le informazioni rilevanti concernenti i dati rilasciati e ricevuti dal TSP, in particolare, allo scopo di fornire prove in procedimenti giudiziari e al fine di garantire la continuità del servizio. In particolare: • Viene mantenuta la riservatezza e l'integrità delle registrazioni correnti e archiviate relative al

funzionamento dei servizi. • Le registrazioni relative al funzionamento dei servizi sono archiviate in modo completo e riservato in conformità con le pratiche commerciali divulgate. • Le registrazioni relative all'esercizio dei servizi sono rese disponibili se richieste al fine di fornire evidenza del corretto funzionamento dei servizi ai fini di procedimenti legali. • Viene registrato l'orario preciso degli eventi ambientali, di gestione delle chiavi e di sincronizzazione dell'orologio significativi del TSP. Il tempo utilizzato per registrare gli eventi come richiesto nel registro di controllo è sincronizzato continuamente con l'UTC. • Le registrazioni relative ai servizi devono

7.14 Business continuity management

TSP definisce e mantiene un piano di continuità da attuare in caso di disastro. In caso di disastro, compresa la compromissione di una chiave di firma privata o la compromissione di qualche altra credenziale del TSP, il guasto di componenti critici del suo sistema affidabile, inclusi hardware e software, le operazioni devono essere ripristinate entro il termine stabilito nel piano di continuità, dopo aver affrontato ogni causa del disastro che potrebbe ripresentarsi con adeguate misure correttive .

7.15 TSA termination and termination plans

Nel caso in cui AGT TSA cessi la propria operatività, ne dà comunicazione preventiva all'Organismo di Vigilanza nazionale AgID.

AGT TSP, a seguito di un aggiornato piano di cessazione, fornisce tempestiva comunicazione a tutti gli affidatari al fine di ridurre al minimo eventuali disservizi che dovessero derivare dalla cessazione dei servizi.

- Il TSP informerà almeno 60 giorni prima della risoluzione i seguenti soggetti: tutti i sottoscrittori e gli altri soggetti con i quali AGT ha accordi o altre forme di rapporti consolidati, tra cui i soggetti affidatari, AGT e le autorità competenti (AgID e l'organismo di certificazione). Inoltre, queste informazioni devono essere messe a disposizione di altre parti di affidamento;

- Il TSP cesserà l'autorizzazione di tutti i subappaltatori ad agire per conto del TSP nello svolgimento di qualsiasi funzione relativa al processo di emissione dei token del servizio fiduciario;
- La TSA manterrà o trasferirà a una parte affidabile i suoi obblighi di rendere disponibile la sua chiave pubblica o il suo certificato alle parti di affidamento per un periodo ragionevole;

7.16 Compliance

AGT Enterprise srl offre i propri servizi nel rigoroso rispetto della Legislazione Applicabile e delle Norme Tecniche. La verifica viene eseguita attraverso audit interni ed esterni. La TSA garantisce in ogni momento il rispetto della legge applicabile. In particolare, la TSA è conforme a:

- Regolamento (UE) 910/2014 ETSI TS 119 421
- IETF (RFC 3161) [7]