Manuale Operativo

Manuale Operativo

Firma Elettronica Avanzata FEA

Firma con Token

Azimut Capital Management SGR S.p.A

Data	1 Ottobre 2016
Versione	1.0
Stato	Definitivo

1 SOMMARIO

2 PREMESSA

Il presente documento riporta le informazioni relative al progetto di Firma Elettronica Avanzata con Token che ha realizzato il Gruppo Azimut. Il progetto di Firma Elettronica Avanzata è stato realizzato per la società del Gruppo Azimut: Azimut Capital Management SGR S.p.A.

3 DEFINIZIONI

3.1 DEFINIZIONI RIGUARDANTI I SOGGETTI

Soggetto	Illustrazione
Certificatore	È l'ente, pubblico o privato, abilitato a rilasciare certificati digitali previa specifica procedura di certificazione in conformità con gli standard nazionali ed europei.
Consulente Finanziario	È la persona incaricata, dal Soggetto che eroga i servizi di Firma Elettronica Avanzata, all'identificazione del Cliente; lo informa in merito alle condizioni d'uso e alle modalità del servizio; partecipa al processo di attivazione della Firma Elettronica Avanzata da parte dell'utente.
Soggetti erogatori dei servizi di Firma Elettronica Avanzata	Sono i soggetti giuridici che erogano soluzioni di Firma Elettronica Avanzata al fine di utilizzarle nei rapporti intrattenuti con soggetti terzi per motivi istituzionali, societari o commerciali, realizzandole in proprio o anche avvalendosi di soluzioni realizzate dai soggetti che le realizzano come attività di impresa.
Soggetti realizzatori dei servizi di Firma Elettronica Avanzata	Sono i soggetti giuridici che, quale oggetto dell'attività di impresa, realizzano soluzioni di Firma Elettronica Avanzata a favore di Soggetti erogatori.
Titolare	E' la persona fisica identificata dal Certificatore, cui è stata attribuita la firma digitale (o remota) ed è stata consegnata la chiave privata del certificatore stesso.
Cliente	È il soggetto a favore del quale la licenziataria mette a disposizione una soluzione di Firma Elettronica Avanzata al fine di sottoscrivere i documenti informatici.

3.2 ACRONIMI, DEFINIZIONI E TERMINI UTILIZZATI

Sigle	Illustrazione
AES	Acronimo di Advanced Encryption Standard è un algoritmo (utilizzato come standard dal governo degli Stati Uniti) di cifratura a blocchi e a chiave simmetrica operante su un gruppo di bit a lunghezza finita.
AgID	Agenzia per l'Italia Digitale (come da Decreto Legislativo 22 giugno 2012 n.83 articolo 22) ha sostituito CNIPA e DigitPa.
CAD	Il codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n.82 e successivi modificazioni.
Certificato digitale	Nella crittografia asimmetrica un certificato digitale è un documento elettronico che attesta l'associazione univoca tra una chiave pubblica e l'identità di un soggetto (una persona, una società, un computer, etc) che dichiara di utilizzarla nell'ambito delle procedure di cifratura asimmetrica e/o autenticazione tramite firma digitale.
Certificato qualificato	Il certificato digitale conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II del medesima direttiva.
Chiave Privata	È la chiave di crittografia utilizzata in un sistema di crittografia asimmetrica al fine di proteggere la firma apposta. La chiave privata è associata a una chiave pubblica ed è in possesso del Titolare che la utilizza per firmare digitalmente i propri documenti.
Chiave Pubblica	E' la chiave crittografica in un sistema di crittografia asimmetrica ed è utilizzata per verificare la firma digitale apposta su un documento informatico dal titolare della chiave asimmetrica. Tale chiave è associata ad una chiave Privata.
CNIPA (DigitPA)	Centro Nazionale per l'Informatica nella Pubblica Amministrazione. E' l'organismo di controllo istituito dal Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri.
Dispositivo sicuro per creazione della Firma	Dispositivo Hardware in grado di proteggere in modo efficace la segretezza della chiave privata.
Dispositivi sicuri per la generazione della Firma Elettronica	Mezzi sui quali il firmatario può conservare un controllo esclusivo la cui conformità è accertata ai sensi dell'art. 12 del DPCM 22/02/2013
Dispositivi sicuri per la generazione della firma Digitale	Mezzi sui quali il firmatario può conservare un controllo esclusivo la cui conformità è accertata ai sensi dell'art. 13 del DPCM 22/02/2013
Documento Informatico	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Sigle	Illustrazione
Documento analogico	La rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.
Duplicato informatico	Documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo su dispositivi diversi, della medesima sequenza di valori binari del documento originario.
Copia informatica di documento informatico	Il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza dei valori binari
Firma Elettronica	L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.
Firma Elettronica Avanzata (FEA)	Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.
Firma Elettronica Qualificata	Un particolare tipo di Firma Elettronica Avanzata che sia basata su un certificato qualificato e realizzata tramite un dispositivo sicuro per la creazione ella firma.
Firma digitale	Particolare tipo di Firma Elettronica basata su un certificato qualificato e su un sistema di chiavi crittografiche, pubblica e privata, correlate tra loro, consentendo al titolare, tramite chiave privata, e al destinatario, tramite chiave pubblica, di rendere manifesta e di verificare la provenienza e l'integrità di uno o un insieme di documenti informatici.
Gestione informatica di documenti	L'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato, effettuato mediante sistemi informatici.
HASH	Funzione matematica che genera, a partire da un'evidenza informatica, un'impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
Marca Temporale (Timestamp)	Riferimento temporale che consente la validazione temporale (data certa) e che dimostra l'esistenza di un'evidenza informatica in un tempo certo.
PAdes	Formato di busta crittografica definito nella norma ETSI TS 102 778 basata a sua volta sullo standard ISO/IEC 32000 e successive modifiche.

Sigle	Illustrazione
PDF	È uno standard aperto per lo scambio di documenti elettronici incluso nella categoria ISO (International Organization for Standardization).
RSA	Algoritmo di crittografia asimmetrica. Questo algoritmo si basa su utilizzo di chiavi pubblica e privata.
SHA-1	Acronimo di Secure Hash Algorithm: identifica un algoritmo che genera un'impronta digitale di 160 bit.
SHA-256	Acronimo di Secure Hash Algorithm: identifica un algoritmo che genera un'impronta digitale di 256 bit.
SHA-512	Acronimo di Secure Hash Algorithm: identifica un algoritmo che genera un'impronta digitale di 512 bit.
Token	E' il PIN CODE inviato all'utente tramite SMS. Il PIN CODE ha valenza temporanea e può essere usato una sola volta. Ogni PIN CODE è associato ad un solo Transaction ID che identifica la richiesta di firma per la quale è stato inviato il PIN CODE
Timbro di Firma	Contiene il Nome e Cognome dell'utente che ha firmato, il Token utilizzato per firmare, il Transaction ID dell'operazione di firma associata al Token
Blob di Firma	Contiene il codice NDG dell'utente che ha firmato, il Nome e Cognome dell'utente che ha firmato, il numero di telefono associato al TOKEN utilizzato per firmare, la data di firma
Soluzioni di Firma Elettronica Avanzata	Soluzioni strumentali alla generazione e alla verifica della Firma Elettronica Avanzata di cui all'art. 1, comma 1, lettera q-bis del CAD

RIFERIMENTI NORMATIVI

Item	Riferimenti	Descrizioni
(0)	**1999/93/CE**	Direttiva del Parlamento Europeo e del Consiglio del 13 dicembre 1999 relativa a una comune visione comunitaria in tema di firme elettroniche.
(1)	**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.
(2)	**D.Lgs. 196/2003**	Decreto Legislativo 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali".
(3)	**D.Lgs. 82/2005**	Decreto Legislativo 7 marzo 2005 N. 82 "Codice dell'amministrazione Digitale".
(4)	**D.Lgs. 4 aprile 2006 n. 159**	Decreto Legislativo 4 aprile 2006 N. 159.Disposizione integrative e correttive al decreto legislativo 7 marzo 2005, n.82, recante codice dell'amministrazione digitale.
(5)	**DPCM 12 ottobre 2007**	Decreto del Presidente del Consiglio dei Ministri 12 ottobre 2007. Differimento del termine che autorizza l'autodichiarazione circa a rispondenza ai requisiti di sicurezza a cui all'art. 13, comma4, del DPCM, pubblicato sulla Gazzetta Ufficiale del 30 ottobre 2003, n. 13.
(6)	**DPCM 30 marzo 2009**	Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009. Il presente decreto abroga il DCPM del 13 gennaio 2004 "Regole Tecniche" in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici. (Gazzetta Ufficiale n. 129 del 6 giugno 2009).
(7)	**D.Lgs. 235/2010**	Decreto Legislativo 30 dicembre 2010 n. 235. Modifiche ed integrazioni al D.Lgs. 7 marzo 2005 n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge n. 69 del 18 giugno 2009. Codice dell'amministrazione digitale pubblicato su Gazzetta Ufficiale n. 6 del 10 gennaio 2011.
(8)	**D.Lgs. n.83 22 giugno 2012**	Decreto Legislativo n. 83 del 22 giugno 2012 Art 22 Sospensione di CNIPA e DigitPA che confluiscono nell'**Ag**enzia per l'**I**talia **D**igitale (AgID).

Item	Riferimenti	Descrizioni
(9)	**D.Lgs. N. 221 17 dicembre 2012**	Decreto Legislativo n. 221 del 17 dicembre 2012 "Misure Urgenti per la crescita del Paese". Il CAD, modificato nell'articolo 21, afferma il principio secondo cui "l'utilizzo del dispositivo di Firma Elettronica Qualificata o Digitale si presume riconducibile al titolare, salvo che questi dia prova contraria". (la FEA è riportata ai metodi di disconoscimento classici del codice di procedura civile Art 214).
(10)	**Regole Tecniche DPCM 22 febbraio 2013**	Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013 "Regole Tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3,24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, 3 e 71.
(11)	**Regolamento UE n. 910/2014**	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

4 GLI ATTORI

4.1 SOGGETTO CHE EROGA LA SOLUZIONE

Azimut Capital Management SGR S.p.A., come da articolo 55 comma 2 lettera a) del Decreto del Presidente del Consiglio dei Ministri datato 22 febbraio 2013, si identifica come Soggetto che eroga la soluzione di Firma Elettronica Avanzata, con Token, al fine di utilizzarla nei rapporti intrattenuti con soggetti terzi (utenti o clienti) per motivi commerciali.

4.1.1 DATI IDENTIFICATIVI

Ragione Sociale	**Azimut Capital Management SGR S.p.A**
Indirizzo sede	Via Cusani 4 – 20121 Milano
Legale Rappresentante	Sergio Albarelli
Codice Fiscale	04631200963
Partita IVA	04631200963
Registro Imprese	Milano
REA	1762051
Capitale Sociale (in Euro)	2.000.000,00 i.v.
Indirizzo E-Mail	info@azimut.it
Numero Telefonico	0288981
Numero FAX	02 88985500
Indirizzo Sito istituzionale	www.azimut.it

4.1.2 ASSISTENZA CLIENTE

Per contattare Azimut Capital Management SGR S.p.A al fine di ricevere informazioni ed assistenza sul servizio di FEA il cliente può:

- Contattare la SGR all'indirizzo postale **Azimut Capital Management SGR S.p.A. Via Cusani 4 20121 Milano;**
- Contattare il Consulente Finanziario di riferimento;
- Chiamare il numero Assistenza ClientiMyAzimut indicato sulla brochure informativa pubblicata sul sito internet di Azimut.

4.2 SOGGETTO CHE REALIZZA LA SOLUZIONE DI FIRMA ELETTRONICA AVANZATA CON TOKEN

In aderenza a quanto espresso nell'Art, 55 comma 2 lettera b) del DCPM datato 22.2.2013, si segnala che il software di Firma Elettronica Avanzata con Token utilizzata da Azimut Capital Management SGR S.p.A è stata realizzata dalla società XYZMO Software GmbH con sede ad Ansfelden in Austria, la soluzione è denominata Click to Sign. XYZMO Software GmbH opera da oltre 10 anni nei sistemi di Firma Elettronica Avanzata.

4.3 ALTRE SOGGETTI COINVOLTI

4.3.1 STUDIO LEGALE ZITIELLO E ASSOCIATI

Studio legale che ha curato la consulenza legale per la **SGR**.

4.3.2 OBJECTWAY FINANCIAL SOFTWARE SPA

Società che realizza la piattaforma di consulenza finanziaria integrando il software di Firma con Token Click to Sign e conserva presso il proprio Data Center i server XYZMO acquistati dalla **SGR** ma dei quali cura installazione, gestione e aggiornamento.

4.3.3 POSTEL SPA

Cura l'attività di archiviazione, apposizione della data certa e conservazione a norma dei documenti digitali sottoscritti con FEA.

4.3.4 ACTALIS SPA

In qualità di Certification Authority fornisce il certificato asimmetrico di crittografia, il certificato non qualificato di firma e la loro installazione. Conserva inoltre le chiavi private di cifratura del certificato utilizzato per crittografare le firme poste sui documenti.

5 SCOPO DEL DOCUMENTO

Questo documento ha lo scopo di descrivere le caratteristiche, le modalità operative, le procedure adottate e le regole predisposte ed utilizzate dagli operatori incaricati dalla **SGR** e dai Clienti della **SGR** al fine di gestire i servizi di Firma Elettronica Avanzata con Token. Il documento recepisce quanto richiesto dalle Regole Tecniche del 22 febbraio 2013.

In particolare sono descritte, nel documento, le procedure atte a soddisfare quanto richiesto in tema di generazione, apposizione e verifica della Firma Elettronica Avanzata, Firma Digitale Remota e Validazione Temporale dei documenti informatici. Sono recepite le indicazioni espresse dal **CAD** e successive modifiche riportate nel D.Lgs. del 30 dicembre 2010, n. 235 e dal DCPM 22 febbraio 2013 (di seguito, le "**Regole Tecniche**").

La **SGR** provvederà annualmente alla verifica della conformità della propria soluzione di Firma Elettronica Avanzata e, ove si renderà necessario, provvederà ad aggiornare questo documento anche in considerazione dell'evoluzione della normativa e degli standard tecnologici.

6 FINALITÀ

Con il progetto di Firma Elettronica Avanzata con Token, la **SGR** intende far sottoscrivere ai clienti interessati in formato digitale moduli, contratti, disposizioni e altri documenti relativi ai prodotti e servizi forniti dalla SGR e dalle società terze con cui ha stipulato apposite convenzioni. Firmare documenti direttamente in formato elettronico utilizzando la Firma Elettronica Avanzata permetterà alla **SGR** di poter digitalizzare i processi cartacei ai fini di una maggiore efficienza, un miglior servizio alla propria clientela ed un maggior rispetto per l'ambiente.

7 QUADRO NORMATIVO

Il processo di **FEA** realizzato rispecchia quanto espresso nella normativa in essere con particolare riferimento al **CAD**.

Sul piano probatorio, l'art. 21, comma 2 del CAD precisa infatti che il documento informatico sottoscritto con firma elettronica avanzata (ma anche qualificata o digitale) – che garantisce determinati requisiti – ha l'efficacia prevista dall'art. 2702 c.c., ossia di scrittura privata.

Inoltre, la nuova formulazione dell'art. 21, comma 2-bis, del CAD recita: "*Salvo quanto previsto dall'articolo 25, le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma*

digitale. Gli atti di cui all'articolo 1350, numero 13) del codice civile soddisfano comunque il requisito della forma scritta se sottoscritti con firma elettronica avanzata, qualificata o digitale".

Il requisito della forma scritta è previsto, a pena di nullità, per i contratti relativi ai servizi di investimento ai sensi dell'art. 23 del d.lgs. 24 febbraio 1998, n. 58 (di seguito "**TUF**").

Il quadro normativo di riferimento è individuabile nelle Regole Tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali.

8 FIRMA CON TOKEN COME FIRMA ELETTRONICA AVANZATA

Per poter essere valida come FEA, la Firma con Token deve garantire il rispetto dei requisiti previsti dall'art. 56 delle Regole Tecniche.

In particolare e a tal fine, la soluzione di firma scelta dalla SGR garantirà:

1) L'identificazione del firmatario del documento;
2) La connessione univoca della firma al firmatario;
3) Il controllo esclusivo del firmatario del sistema di generazione della firma
4) La possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma;
5) La possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;
6) L'individuazione del soggetto di cui all'articolo 55, comma 2, lettera (a) delle Regole Tecniche;
7) L'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificare gli atti, fatti o dati nello stesso rappresentati;
8) La connessione univoca della firma al documento sottoscritto;

Nello specifico, il processo disegnato per la **SGR** rispecchia i punti elencati e, di conseguenza, la Firma con Token adottata si configura come Firma Elettronica Avanzata

A tale fine, la **SGR** per rispondere positivamente a quanto richiesto, ha adotta le seguenti misure:

Identificazione del firmatario del documento	L'utente che intende firmare il documento si deve collegare alla sua area riservata MyAzimut tramite le credenziali personali che solo lui può conoscere e di cui è responsabile.
Connessione univoca della firma con il	L'utente può apporre la firma solo dove è previsto che sia lui a

firmatario	firmare. Il Token da utilizzare per la firma, ha una validità temporanea e viene inviato esclusivamente al numero di telefono che il cliente stesso ha comunicato in fase di sottoscrizione del Servizio Firma Elettronica Avanzata con Token o di cui ha richiesto una variazione in una fase successiva tramite apposito modulo di variazione dati contrattuali.
Controllo esclusivo del firmatario del sistema di generazione della firma	La firma apposta unisce 3 strumenti che sono sotto il diretto controllo del firmatario (numero di telefono su cui ricevere il Token, il Token temporaneo e l'accesso all'area riservata MyAzimut). Inoltre il firmatario può sempre: scorrere il documento; confermare la firma apposta; cancellare la firma apposta e ripetere la firma; annullare l'operazione di firma.
Possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma	L'integrità del documento è garantita dal processo che prevede l'apposizione di una firma informato PAdEs con contestuale generazione di Hash. Esiste sempre la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma. Presso il sito dell'Agenzia per l'Italia Digitale (URL http://www.agid.gov.it/identitadigitali/firme-elettroniche/software-verifica) sono disponibili gratuitamente software per la verifica dell'integrità del documento in conformità alla delibere CNIPA del 21 maggio 2009 num.45, è altresì possibile esigere la verifica con Adobe Acrobat Reader.
Possibilità per il firmatario di ottenere evidenza di quanto sottoscritto	Il firmatario ha la visione completa del documento sottoposto a firma e può scorrerlo per l'esamina. Oltre a ciò il processo prevede la consegna della copia de documento firmato ovvero con trasmissione elettronica o via email o con accesso ad un'area riservata sicura.
Individuazione del soggetto di cui all'art. 55, comma 2, lettera (a)	La **SGR** è identificabile come soggetto proponente e ha previsto tutto quanto necessario nel rispetto del requisiti previsti dall'art. 55 comma 2 lettera (a)
Assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificare gli atti, fatti o dati nello stesso rappresentati	Il documento generato nel processo di firma è nel formato PDF e chiuso con certificato riconducibile alla **SGR**.
Connessione univoca della firma al documento sottoscritto	Il processo previsto consente quanto richiesto attraverso la generazione di Hash al momento della firma, questi possono essere utilizzati poi in fase di verifica e controllo. La connessione univoca è garantita dalla soluzione adottata SIGNificant che utilizza algoritmi di cifratura collegate all'impronta del documento

9 OBBLIGHI

I soggetti che erogano soluzioni FEA (la **SGR**) hanno una serie di obblighi al fine di garantire il rispetto di tutti i requisiti richiesti dalla normativa di settore sopra menzionata. Tali requisiti sono riepilogati di seguito, mentre nei paragrafi successivi si illustrano dettagliatamente le modalità utilizzate dalla SGR per garantirne il rispetto.

1) Identificare in modo certo l'utente tramite un valido documento di riconoscimento;
2) Informare l'utente in relazione agli esatti termini e condizioni d'uso del servizio, compresa ogni eventuale limitazione d'uso;
3) Subordinare l'attivazione del servizio alla sottoscrizione di una dichiarazione di accettazione delle condizioni del servizio da parte dell'utente;
4) Conservare per almeno **20 anni** copia del documento di riconoscimento e la dichiarazione del punto 3;
5) Garantire la disponibilità, integrità, leggibilità e autenticità del documento di accettazione del servizio (punto 3);
6) Fornire liberamente e gratuitamente copia della dichiarazione e le informazioni di cui al punto 3) al firmatario su sua richiesta;
7) Rendere note le modalità con cui effettuare la richiesta di cui al punto 6), pubblicandole anche sul proprio sito internet;
8) Rendere note le caratteristiche del sistema realizzato atte a garantire quanto prescritto dalle Regole Tecniche articolo 56, comma 1;
9) Specificare le caratteristiche delle tecnologie utilizzate e come queste consentono di ottemperare a quanto prescritto;
10) Prevedere la possibilità di revoca del servizio da parte del cliente/utente.

9.1 IDENTIFICAZIONE DEL FIRMATARIO

L'identificazione del firmatario (Cliente) viene effettuata dagli operatori incaricati della **SGR** (Promotori Finanziari) e, a tal fine, vengono richiesti documenti di identità e codice fiscale. Tutti i documenti debbono essere in corso di validità.

Per quanto concerne i documenti di riconoscimento, come da articolo 35 del DPR 445/2000, sono considerati validi i seguenti:

- ✓ Carta d'identità
- ✓ Passaporto
- ✓ Patente di Guida
- ✓ Patente Nautica
- ✓ Libretto della Pensione
- ✓ Patentino di abilitazione alla conduzione di impianti termici
- ✓ Porto d'Armi

In alternativa è possibile utilizzare altre tessere di riconoscimento purché presentino fotografia e timbri di validazione e siano rilasciate da una Amministrazione delle Stato.

Il codice fiscale può essere reperito da documenti rilasciati dall'Agenzia delle Entrate. Ad oggi risultano validi: Codice fiscale sia in forma cartacea o tesserino plastico; Tessera Sanitaria.

9.2 INFORMARE L'UTENTE FIRMATARIO

I promotori finanziari, in qualifica di operatori della **SGR**, prima di procedere con la richiesta di accettazione dell'utilizzo del servizio FEA, procedono a informare il firmatario (Cliente) in relazione alla finalità (come espresso nel capitolo 6) le limitazioni d'uso (capitolo 7). Viene anche presentata e, se richiesta, consegnata, informativa dettagliata per l'utilizzo del servizio.

9.3 DICHIARAZIONE DI ACCETTAZIONE

I promotori finanziari della **SGR** dopo aver adeguatamente informato il firmatario (Cliente), chiedono la sottoscrizione della dichiarazione di accettazione delle condizioni di erogazione del servizio da parte del cliente. Tale documento riporta tutti i dati informativi del cliente, la descrizione del servizio e richiede firme analogiche su documento cartaceo per l'accettazione del servizio e modifiche di rapporto.

9.4 CONSERVAZIONE DOCUMENTI RICHIESTI

In pieno rispetto di quanto previsto nell'articolo 56 comma 1 del DPCM 22/02/2013, al fine di dare evidenza di quanto previsto, si eseguono copia del documento di riconoscimento e del codice fiscale. Queste copie, in allegato al documento di accettazione del servizio, verranno conservate per almeno 20, anni dalla **SGR** garantendone, per tutto il periodo richiesto la disponibilità, integrità e leggibilità.

9.5 GARANZIA DI DISPONIBILITÀ, INTEGRITÀ E LEGGIBILITÀ DEL DOCUMENTO DI ACCETTAZIONE DEL SERVIZIO E MESSA A DISPOSIZIONE GRATUITA DEL DOCUMENTO DI ACCETTAZIONE

Su richiesta del firmatario (Cliente) effettuata mediante comunicazione scritta, la **SGR** si rende disponibile a fornire, senza oneri per il firmatario, copia cartacea della dichiarazione di accettazione da parte del Cliente stesso delle condizioni e dei termini del Servizio oltre alle copie dei documenti firmati con FEA e conservati in copia informatica al solo scopo di informazione.

Il Cliente potrà contattare il proprio consulente finanziario o direttamente la SGR per ricevere assistenza per attivare la richiesta.

9.6 CARATTERISTICHE DEL SISTEMA DI FIRMA

Al fine di ottemperare alla normativa di cui articolo 56 comma 1, la **SGR**, nel paragrafo 12 descrive le misure adottate a garanzie di quanto prescritto.

9.7 LA TECNOLOGIA UTILIZZATA

Nel paragrafo 13, la **SGR**, descrive in modo dettagliato le caratteristiche hardware e software al fine di ottemperare quanto richiesto dalle Regole Tecniche DPCM 22/02/2013.

9.8 PUBBLICAZIONE SUL SITO

La **SGR**, in ottemperanza a quanto richiesto dalla normativa in essere, ha pubblicato sul sito internet www.azimut.it il presente documento che descrive anche le caratteristiche del sistema di firma e le caratteristiche delle tecnologie utilizzate.

9.9 SERVIZIO DI REVOCA

Il processo di Firma Elettronica Avanzata adottato dalla **SGR** permette la revoca dei servizi tramite apposita richiesta scritta da parte del cliente. In caso di revoca la FEA non potrà più essere utilizzata.

Il cliente potrà contattare il proprio consulente finanziario o direttamente la SGR per ricevere assistenza per attivare le richiesta di Revoca.

10 TUTELA ASSICURATIVA

Ulteriore richiesta espressamente citata nelle Regole Tecniche, prevede una copertura assicurativa a garanzia del firmatario.

Il soggetto che eroga soluzioni di Firma Elettronica Avanzata si impegna a stipulare una polizza assicurativa per la copertura dei rischi dell'attività svolta e dei danni a tutela delle parti (Firmatari ed i Terzi) per almeno Euro 500.000,00(cinquecentomila/00).

La **SGR**, in qualità di soggetto che eroga la soluzione di Firma Elettronica Avanzata, ha stipulato polizza assicurativa con primaria compagnia Assicurativa per la copertura dei suddetti rischi.

11 LA SOLUZIONE AZIMUT

In tema di firma con Token, XYZMO ha prestato particolare attenzione alla sicurezza del dato di firma. Infatti, mentre il firmatario esegue la firma, i dati che caratterizzano la firma ovvero il Blob di Firma sono cifrati nella memoria del dispositivo mobile con la chiave simmetrica AES, la cui chiave a sua volta è cifrata con la chiave pubblica l'algoritmo asimmetrico RSA.

Il firmatario ha il controllo esclusivo del processo di firma disponendo di una serie di funzioni e può:

- Scorrere il documento senza limitazioni al fine di poter aver evidenza di quanto da lui sarà sottoscritto;
- Selezionare l'area di firma su cui vuole firmare
- Inserire nell'apposita area di firma selezionata il Token inviato tramite SMS;
- Modificare il Token inserito qualora si accorga di averlo inserito in maniera errata
- Richiedere nuovamente un nuovo Token qualora abbia cancellato per errore l'SMS inviato o qualora non sia arrivato l'SMS
- Annullare l'operazione di firma, qualora non voglia più firmare, con la selezione della funzione **ANNULLA**;
- Confermare la firma apposta con la selezione della funzione **OK**;
- Completare il processo di firma del documento con la selezione della funzione **CHIUDI**
- Annullare il processo di firma del documento qualora non sia più propenso a firmare, con la seleziona della funzione **CANCELLA**.

Con la conferma (funzione **OK**) da parte del firmatario alla firma apposta, il SIGNificant Client invia il Blob di Firma al SIGNificant Server che calcola l'impronta del documento con l'algoritmo SHA.

I dati cifrati, la chiave ASE cifrata, e l'impronta (HASH) del documento, sono inseriti nel documento PDF, alla fine del processo di firma del documento il SIGNificant Server firma il documento in standard PAdES, secondo la deliberazione CNIPA 21 maggio 2009, n.45.

Quest'ultima firma, garantisce l'integrità (documento non alterato) e autenticità (autore) del documento digitale (gruppo Azimut).

I dati così protetti non possono essere decriptati, visualizzati ed esaminati. Unica possibilità è di poter disporre della chiave privata, chiave in possesso solo di ente terzo e con regole di consegna solo per particolari eventi, e di un apposito software di analisi.

Questa operazione è prevista come processo di gestione di eventuali contenziosi.

11.1 IL SOFTWARE DI FIRMA

Per la realizzazione del servizio di Firma Elettronica Avanzata con Firma Token, **Azimut Capital Management SGR S.p.A** ha utilizzato un software denominato Click to Sign di Xyzmo il cui client è installato sulla postazione mobile e Web dei clienti della SGR.

La soluzione di Xyzmo mette a diposizione, per questo progetto, le componenti: SIGNificant Server; SIGNificant Client ed Identity Server.

11.2 IL SIGNIFICANT CLIENT

E' la componente inclusa nell' APP iOS ed Android installata sui dispositivi Mobile e sulla component Web presente nei PC del firmatario (Cliente) ed ha il compito di ricevere e visualizzare i documenti da sottoporre all'utente firmatario, di acquisire il Token temporaneo, di cifrarli insieme ad altre informazioni (chiave AES cifrata) e di inviarli al SIGNificant Server.

Il SIGNificant Client, per la cifratura delle informazioni, utilizza due differenti algoritmi di cifratura, un primo algoritmo di cifratura simmetrica AES-256 per cifrare i dati che caratterizzano la firma ovvero il Blob di Firma; un secondo algoritmo di cifratura asimmetrica RSA (chiave pubblica) per cifrare la chiave AES-256. La chiave AES-256 è generata in maniera casuale da SIGNificant Client per ogni firma. La chiave pubblica di cifratura utilizzata dall'algoritmo RSA è compilata insieme al SIGNificant Server e SIGNificant Client.

11.3 IL SIGNIFICANT SERVER

E' il server di gestione dell'attività di firma, installato presso ObjectWay, riceve il documento in formato PDF dal SIGNificant Client, lo trasforma in immagine ottimizzata e lo invia al SIGNificant Client.

Il SIGNificant Client dopo aver acquisito i dati che caratterizzano la firma li invia cifrati al SIGNificant Server**,** il SIGNificant Server verifica la corrispondenza, inserisce il Blob di Firma del firmatario e la chiave AES cifrata nel documento ed invia al SIGNificant Client l'esito positivo dell'inserimento della firma.

Con la conferma da parte del SIGNificant Client della conclusione delle operazioni di firma il SIGNificant Server rende il documento non modificabile grazie all'apposizione di certificato di chiusura, rilasciata da una Certification Authority accreditata presso AgID.

Il SIGNificat Server utilizza l'algoritmo di cifratura simmetrica SHA-512 per calcolare l'impronta del documento informatico e l'algoritmo RSA per firmare digitalmente i documenti.

11.4 L'IDENTITY SERVER

E' il server che conserva l'associazione Utente e Numero di Cellulare cui inviare via SMS il Token per la firma.

L'Identity Server, dopo avere ricevuto dal SIGNificant Client la richiesta di firma del firmatario, verifica se il firmatario ha un numero di telefono associato, genera il Transaction ID di firma con il Token per firmare e invia il Token al numero di telefono associato al firmatario.

Dopo che il firmatario ha selezionato la funzione OK sulla maschera di firma, l'Identity Server verifica che il Token inserito dal firmatario nel punto firma sia corrispondente con il Transaction ID assegnato.

11.5 MODALITÀ DI FIRMA

La soluzione adottata si basa sulla tecnologia Xyzmo e su una architettura che prevede l'installazione di una specifica APP sui dispositivi Mobile disponibile sugli Store Apple ed Android e una applicazione WEB rivolta ai clienti del gruppo AZIMUT. Tali applicazioni permettono l'utilizzo della logica del SIGNificant Client di Xyzmo che comunica, solo in modalità On-Line e su canale sicuro HTTPS, con il SIGNificant Server di Xyzmo e l'Identity Server.

La prima attività che viene richiesta al cliente, in modo che possa poi usufruire del servizio di Firma Elettronica Avanzata con Token, è l'accettazione e sottoscrizione del consenso all'utilizzo della FEA. Tale consenso viene raccolto dal Consulente dopo aver fatto leggere, illustrato e consegnato l'informativa al cliente.

Per la sottoscrizione di documenti digitali da parte dei clienti, è necessario che gli stessi abbiano inserito le proprie credenziali d'accesso alle applicazioni App o Web, e devono essere stati riconosciuti dal sistema informativo MyAzimut della SGR.

Al firmatario (Cliente) sono sottoposti documenti digitali in formato PDF con uno o più campi firma; il campo firma viene presentato al firmatario in modalità esplicita sulle applicazioni e l'intero foglio del documento è disponibile e visualizzato sullo stesso.

Il Firmatario firma grazie all'inserimento del Token inviato tramite SMS, l'utente mantiene il controllo esclusivo dell'operazione di firma, premendo il tasto OK accetta l'invio dei dati crittografati che verranno poi inseriti sul documento opportunamente protetto.

I dati sono acquisiti dal SIGNificant Client, cifrati, ed inviati al SIGNificant Server su un canale sicuro (HTTPS) che li inserisce nel documento.

A conclusione del processo di firma viene richiesta una conferma alla chiusura del documento con conferma delle firme. In caso di conferma il documento viene chiuso con un certificato non qualificato di chiusura a nome dell'azienda. Il documento chiuso con il certificato di chiusura viene poi messo a

disposizione del servizio di archiviazione e conservazione a norma fornito da Postel. In caso di non conferma, il documento viene cancellato dalla memoria del sistema operazioni di riscrittura su cache da parte dell'applicazione.

11.6 LA SICUREZZA

In tema di firma con Token, XYZMO ha prestato particolare attenzione alla sicurezza del dato di firma. Infatti, mentre il firmatario esegue la firma, i dati che caratterizzano la firma ovvero Il Blob di Firma sono cifrati con la chiave simmetrica AES, la cui chiave a sua volta è cifrata con la chiave pubblica l'algoritmo asimmetrico RSA.

Il firmatario ha il controllo esclusivo del processo di firma disponendo di una serie di funzioni e può:

- Scorrere il documento senza limitazioni al fine di poter aver evidenza di quanto da lui sarà sottoscritto;
- Selezionare l'area di firma su cui vuole firmare
- Inserire nell'apposita area di firma selezionata il Token inviato tramite SMS;
- Modificare il Token inserito qualora si accorga di averlo inserito in maniera errata
- Richiedere nuovamente un nuovo Token qualora abbia cancellato per errore l'SMS inviato o qualora non gli sia arrivato l'SMS
- Annullare l'operazione di firma, qualora non voglia più firmare, con la selezione della funzione **ANNULLA**;
- Confermare la firma apposta con la selezione della funzione **OK**;
- Completare il processo di firma del documento con la selezione della funzione **CHIUDI**
- Annullare il processo di firma del documento non sia più propenso a firmare, con la seleziona della funzione **CANCELLA**.

Con la conferma (funzione **OK**) da parte del firmatario alla firma apposta il SIGNificant Client invia i dati al SIGNificant Server che calcola l'impronta del documento con l'algoritmo SHA.

I dati cifrati, la chiave ASE cifrata, e l'impronta (HASH) del documento, sono inseriti nel documento PDF, alla fine del processo di firma del documento il SIGNificant Server firma il documento in standard PAdES, secondo la deliberazione CNIPA 21 maggio 2009, n.45.

Quest'ultima firma, garantisce l'integrità (documento non alterato) e autenticità (autore) del documento digitale (gruppo Azimut).

I dati così protetti non possono essere decriptati, visualizzati ed esaminati. Unica possibilità è di poter disporre della chiave privata, chiave in possesso solo di ente terzo e con regole di consegna solo per particolari eventi, e di un apposito software di analisi.

Questa operazione è prevista come processo di gestione di eventuali contenziosi.

11.7 INTEGRITÀ DEL DOCUMENTO SOTTOSCRITTO

L'integrità del documento sottoscritto dall'utente è garantita dal certificato riconducibile alla SGR opposto in chiusura di documento.

L'apposizione della firma elettronica è gestita dal SIGNificant Server.

Il SIGNificant Server al termine dell'inserimento dei dati di firma cifrati nel documento, calcola l'impronta con la chiave privata del certificato non qualificato, cifra l'impronta e la inserisce nel documento. Il risultato del processo è la firma del documento che ne garantisce l'integrità e autenticità.

La verifica dell'integrità ed autenticità del documento può essere svolta da un qualsiasi software di verifica conforme al CAD; ad esempio ADOBE ACROBAT READER.

La verifica dell'autenticità della sottoscrizione (la firma) dell'utente può essere eseguita solo quando si è in possesso della chiave privata di cifratura.

La chiave privata di cifratura è conservata presso un ente terzo fidato, **Actalis** in questo caso, che renderà disponibile la chiave solo su motivata (es. l'autorità giudiziaria) richiesta del legale rappresentante.

12 PROCESSO DI IDENTIFICAZIONE E FIRMA

Quando il consulente finanziario richiede al Cliente di apporre una o più firme con Token, può verificare se il Cliente ha già sottoscritto la dichiarazione di accettazione (come da paragrafo 10.3). Se risulta che il Cliente ha già sottoscritto la dichiarazione di accettazione, il consulente potrà procedere.

Se non risulterà che tale operazione sia stata sottoscritta ma il Cliente dichiara di averlo fatto (l'avvenuta sottoscrizione sarà disponibile su sistema dopo i controlli del back office) non si potrà procedere che con forma cartacea sino a che la verifica del back office non sia conclusa.

In ipotesi che non sia mai stata presentata la soluzione e, di conseguenza, mai sottoscritta, il consulente finanziario provvede ad informare in modo chiaro e completo il sottoscrittore come indicato nei paragrafi 10.2 e 10.3 e riportati nel modulo di accettazione. Richiederà i documenti previsti per l'attivazione del servizio di FEA con Token (come illustrato nel paragrafo 10.1), richiederà al cliente la sottoscrizione autografa della dichiarazione di accettazione come descritto nel paragrafo 10.3 e, successivamente, provvederà all'inoltro al back office dei documenti per la loro conservazione come da paragrafo 10.4.

L'utente potrà procedere, dopo che il back office avrà registrato la sua accettazione, a firmare tutti documenti proposti dalla **SGR** su documenti informatici, avendo la stessa efficacia della forma scritta (paragrafo 7).

12.1 ACCETTAZIONE DEL CLIENTE DEL SERVIZIO DI FIRMA ELETTRONICA AVANZATA CON TOKEN

In questa fase, il consulente, provvede ad informare, dando piena disponibilità della documentazione prodotta dal gruppo Azimut, al processo di sottoscrizione con FEA con Token. E' in questa fase che, se il cliente conferma di voler utilizzare questa modalità di firma, il consulente acquisisce la sottoscrizione, **su modulo cartaceo**, del consenso del cliente all'utilizzo della FEA e delle copie dei documenti da allegare.

I dati di:

- Numero di Telefono su cui il Cliente riceve il Token con cui firmare
- E-mail su cui il Cliente riceve le comunicazioni di disponibilità dei documenti ai fini della firma nell'area riservata (Area Firma) presente su MyAzimut

sono riportate all'interno dello stesso modulo cartaceo (Contratto Unico dei Servizi Digitali) che il Cliente sottoscrive per l'adesione al servizio di Firma Elettronica Avanzata di tipo Token. Ogni variazione degli stessi può avvenire solo attraverso la sottoscrizione di un modulo cartaceo di modifica dati contrattuale da parte del Cliente, reso disponibile dalla SGR nella piattaforma MyAzimut; modulo che successivamente dovrà pervenire alla strutture di back-office per le opportune verifiche prima di recepire la richiesta di modifica.

12.2 IL PROCESSO DI FIRMA

I SIGNificant Client, SIGNificant Server e l'Identity Server sono in grado di firmare documenti in formato PDF con Firma Elettronica Avanzata con Token, ciò garantisce che un qualsiasi documento che può essere stampato può anche essere firmato.

Il processo di firma può essere sinteticamente descritto come segue:

- Il consulente, tramite Web o il dispositivo mobile, si identifica al sistema MyDesk della SGR ed esegue l'accesso al sistema informativo del Gruppo Azimut con le proprie credenziali;
- Il consulente compila ed invia in Area Firma condivisa con il Cliente il documento che desidera far sottoscrive al cliente;
- Il cliente, tramite Web o il dispositivo mobile, si identifica al sistema MyAzimut della SGR ed esegue l'accesso al sistema informativo del Gruppo Azimut con le proprie credenziali
- Il cliente accede alla propria Area Firma presente su MyAzimut e seleziona il documento che intende sottoscrivere
- Il documento PDF selezionato dal cliente viene inviato al SIGNificant Server;
- Il SIGNificant Server calcola l'impronta (HASH) del documento, ed invia al SIGNificant Client l'immagine PDF ottimizzata del documento;
- Il documento è visualizzato sul web o sul dispositivo mobile del cliente che attiva il processo di firma.

Il Cliente o sottoscrittore ha il controllo esclusivo del processo di firma e dispone delle seguenti funzioni:

- Visualizzazione del documento in modo da aver evidenza di quanto da lui sarà sottoscritto;
- Inserimento del Token nell'apposita area di firma;
- (**OK**) per confermare l'inserimento;
- (**ANNULLA**) per non procedere con l'inserimento del Token;
- (**CHIUDI**) per completare la firma del documento
- (**CANCELLA**) per annullare la firma del documento.

Mentre il sottoscrittore esegue la firma, i dati che caratterizzano la stessa sono cifrati con la chiave simmetrica AES, la cui chiave a sua volta è cifrata con la chiave pubblica l'algoritmo RSA (a chiavi asimmetriche).

Con la conferma (**OK**) da parte del firmatario il SIGNificant Client invia al SIGNificant Server, i dati della firma cifrati (Blob di Firma), la chiave AES cifrata. Il SIGNificant Server:

- Inserisce i dati ricevuti dal SIGNificant Client nel documento PDF originale residente sul server;
- Invia al SIGNificant Client l'immagine PFD ottimizzata del documento, con il Timbro di firma in bella vista.
- Il SIGNificant Client al ricevimento dell'immagine PDF ottimizzata se i sottoscrittori sono più di uno, o sono richieste più firme dello stesso soggetto, ripeterà le operazioni sopra descritte per un numero di volte necessarie.
- Il SIGNificant Client inoltra la conclusione della sottoscrizione del documento da parte dell'utente al SIGNificant Server.
- Il SIGNificant Server calcola l'impronta (HASH), cifra l'impronta e la inserisce nel documento. Il risultato del processo è la firma in formato PAdES del documento che ne garantisce l'integrità ed autenticità.
- Il SIGNificant Server invia al SIGNificant Client l'immagine PDF ottimizzata del documento firmato digitalmente.
- Il SiGNificant Server chiude il documento con un certificato non qualificato intestato alla società ovvero richiede la firma digitale remota per la chiusura del documento.
- Successivamente vengono chiamati opportuni Web Service per inviare il documento al servizio di archiviazione e conservazione a norma. Tale invio avviene a mezzo di web service, con trasmissione in sicurezza via https, a Postel ente di archiviazione e conservazione a norma. La chiamata via Web Service prevede il passaggio del documento firmato (criptato e chiuso con certificato aziendale) ed una serie di metadati per il controllo del documento. La Web Service ritornerà un esito che potrà essere OK (documento ricevuto correttamente, non corrotto e con tutti i metadati significativi presenti, validati e archiviato da Postel) e un codice MIDA contenente anche il riferimento del documento archiviato; ovvero riceverà un esito KO in presenza di documento corrotto, non conforme o mancanza di corrispondenza nei metadati. In caso di esito KO il documento viene cancellato e l'operazione deve essere ripetuta dall'inizio. L'operazione di inoltro è stimata in 10 millisecondi.

Successivamente vengono rese disponibili le copie elettroniche immagine del documento firmato al cliente, al consulente ed al backoffice (o via WebService o in area riservata sicura chiamata Documenti).

12.3 LE COMUNICAZIONI CIFRATE

La comunicazione ed il trasferimento dei dati di firma tra il Client ed il Server sono su un canale HTTPS (criptato) con algoritmo asimmetrico. Questo protocollo, largamente utilizzato dai sistemi WEB, rende impossibile l'intercettazione dei contenuti in quanto si crea un canale di comunicazione criptato tra Client e Server attraverso lo scambio di certificati, una volta stabilita la connessione al suo interno è utilizzato il protocollo HTTP per l'invio e la ricezione dei dati.

Anche la comunicazione per l'invio del documento ottimizzato ed il trasferimento dei dati di firma tra il Client ed il Server sono su un canale HTTPS (criptato) con algoritmo asimmetrico.

13 ALTRI COMPONENTI

Per la realizzazione di un processo di firma in piena conformità con le Regole Tecniche emesse il 22/02/2013 con Decreto del Presidente del Consiglio dei Ministri, sono necessari i componenti obbligatori alcuni e opzionali altri, di seguito descritti.

13.1 CHIAVE PUBBLICA DI CIFRATURA

I dati di firma sono cifrati utilizzando una chiave asimmetrica generata dal software di firma, questa chiave è cifrata con chiave pubblica di cifratura. La chiave pubblica è compilata da XYZMO insieme al programma SIGNificant Cliente e sono generate da Actalis SPA in qualità di Certification Authority accreditata presso AgDI.

13.2 CHIAVE PRIVATA DI CIFRATURA

La chiave privata, unica in grado di estrarre in chiaro i dati di firma è generata da Actalis SPA in qualità di Certification Authority accreditata presso AgDI. Successivamente la chiave privata sarà conservata presso Actalis SPA in qualità di ente terzo. L'ente terzo sarà chiamato, in fase di eventuale contenzioso, dall'autorità giudiziaria seguendo il processo previsto per la gestione del contenzioso e illustrato in questo documento.

13.3 CERTIFICATO DI FIRMA

Il certificato di firma è installato sul SIGNificant Server ed è utilizzato al termine del processo di Firma Elettronica Avanzata, al fine di garantirne l'integrità (documento non alterato) ed autenticità del documento digitale.

13.4 MARCA TEMPORALE

Il software SIGNificant Server è in grado, qualora richiesto, di inserire nei documento sottoscritti digitalmente marche temporali (TIMESTAMP) conformi alla standard ISO 8601. La marca temporale è il risultato della procedura informatica con cui si attribuiscono, ai documenti informatici, una data ed un orario opponibili a terzi.

14 COMPONENTI DI SICUREZZA

14.1 SERVER

La soluzione applicativa e il software di Xyzmo sono installati su server dedicati ad **AZIMUT** gestiti nei Data Center di **Objectway** che garantiscono gli aspetti di disaster & recovery.

In relazione alle misure di sicurezza adottate il personale di **Objectway** dichiara che sono state messe in atto le misure minime richieste dall'allegato B del Codice Privacy.

In particolare i server non sono esposti all'esterno, la comunicazione è via https, gli accessi sono registrati su appositi log. **Objectway** ha predisposto apposito documento che illustra tutte le misure adottate recepito come allegato della Relazione Tecnica.

15 ARCHIVIAZIONE E CONSERVAZIONE A NORMA DEI DOCUMENTI

Il processo di archiviazione, apposizione della data certa e conservazione a norma è a carico di Postel che provvederà alla stesura del "Manuale di Conservazione" e assumerà la responsabilità della conservazione a norma per le sue componenti.

Per realizzazione di quanto previsto contrattualmente, Postel, mette a disposizione il sistema di archiviazione denominato "Documentum" ed il sistema "AOS" per l'archiviazione a norma.
Tutta l'operatività è posta in sicurezza e, di seguito, sono riassunte alcune caratteristiche tecniche.

Il sistema messo a disposizione da Postel è denominato GED Postel.

Il sistema GED prevede la seguente architettura fisica:

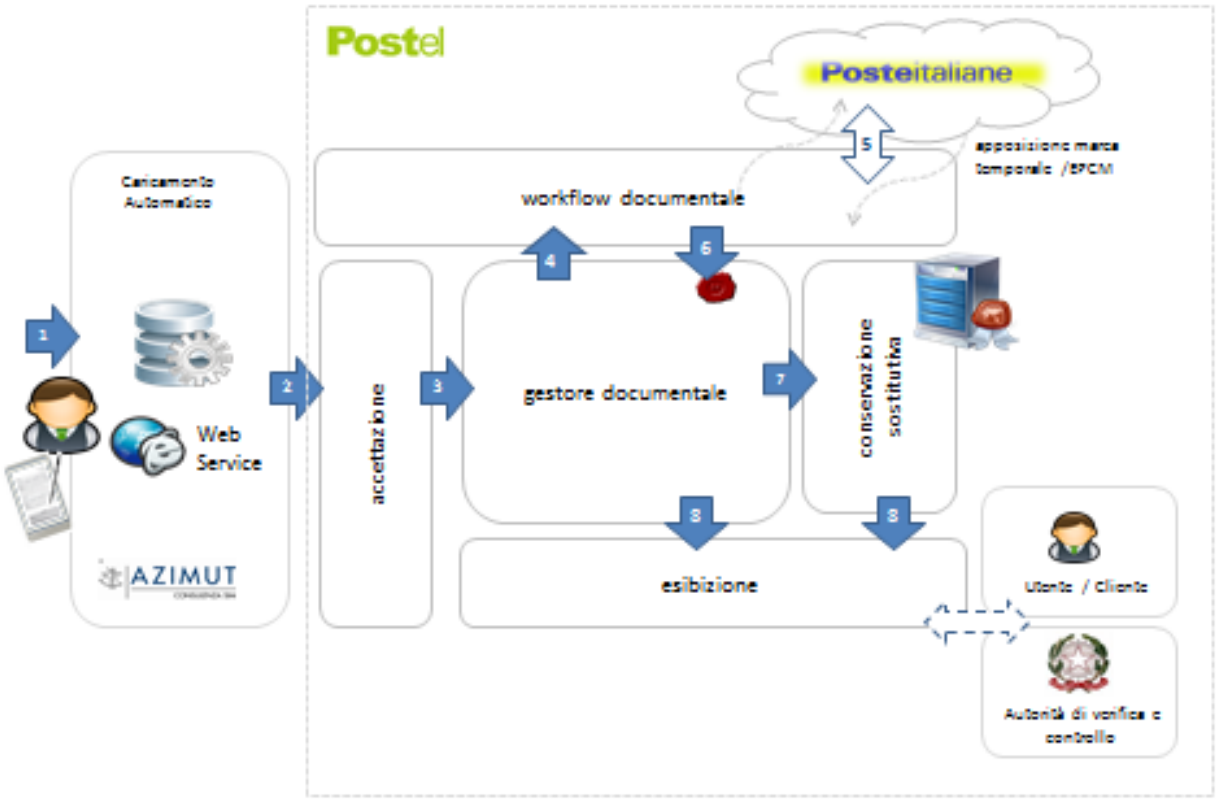
- Reverse Proxy IBM http Server 6.1, Apache web server (RP1),
- Data Server Oracle 10G in alta affidabilità (PB1, PB2),
- Content Serve con SO Red Hat Enterprise Linux 5.0 (CS1,CS2),
- Application Server con SO Red Hat Enterprise Linux 5.0 e Web Server IBM WS 6 (WS1, Ws2),
- Storage dati di tipo SAN (NAS (EMC DMX), EMC Centera,
- Client Acquisizione con SO Windows 2003 (OP1),
- Image Processing Component Server con SO Windows 2003 (IPCS1, IPCS2).

Il processo di archiviazione e conservazione dei documenti firmati è uno dei punti di attenzione del progetto. La regolamentazione per la protezione dei dati che presentano rischi specifici, come nel caso dei dati di firma elettronica avanzata, richiedono che i dati siano archiviati in sicurezza e in nessun punto del processo ci sia la possibilità di manipolazione dei dati. Per questo motivo, il gruppo Azimut, ha scelto di affidarsi a Postel.

Il processo delineato prevede che il documento firmato e chiuso con firma remota qualificata, venga inviato direttamente a Postel a mezzo di web service concordata. Postel marcherà temporalmente (con timestamp) il documento e ne creerà lotto per la conservazione a norma. Immagine del documento sarà disponibile su portale Postel agli utenti Azimut abilitati.

In sintesi il Processo si articola come di seguito:

- L'applicazione, dopo la chiusura del documento invoca una web service (via https) di Postel passando il documento sottoscritto, criptato e chiuso con un certificato intestato a Azimut Holding Spa. Oltre al documento vengono passati dei metadati che servono alla creazione degli indici del documento.
- L'applicazione di Postel esegue delle verifiche in merito alla congruenza dei metadati e di validità del documento ricevuto. Eseguito il controllo ritorna esito OK o KO a seconda dell'esito delle verifiche. Il codice MIDA di risposta, oltre all'esito, riporta anche la tipologia di errore ed identificativo del file per eventuali richiami del documento.
- Se la risposta è OK il documento viene archiviato nel sistema di archiviazione "Documentum" per poi procedere sino al processo di Archiviazione Ottica Sostitutiva a Norma.
- A timing prefissati il sistema documentale provvede a richiedere e marcare, con timestamp, ogni documento ricevuto, inoltrando poi tutti i documenti marcati al sistema di archiviazione e al sistema di Conservazione digitale a norma (AOS) .



Il sistema di archiviazione “Documentum” sarà la momentanea area di staging, prima di ottenere il TimeStamp (dalla CA) per poi passare immediatamente su sistema di Archiviazione a Norma (AOS) dove saranno conservati i file originari.

Gli operatori di Azimut (preventivamente segnalati e registrati, possono accedere al sistema di archiviazione per consultazione produzione di report statistici attraverso Il Portale Postel con l’accesso web denominato Taskspace. Esistono profilazioni diverse per le modalità di consultazione dei documenti (visore, base o supervisore).

L’utente “Visore”, con cui sono stati configurati gli user di Azimut, può soltanto consultare i documenti archiviati e conservati digitalmente, esibire a norma i documenti conservati e accedere alla reportistica.

I documenti originali presenti nel sistema di conservazione, possono essere richiesti in via ufficiale, utilizzando una richiesta formale e a mezzo di scritto, a Postel con firma di autorizzazione del Responsabile dell’archiviazione di Azimut e eventualmente dal rappresentante legale con motivazioni dichiarate e secondo un processo autorizzativo che sarà definito. Postel, su richiesta Azimut, produrrà un Dvd con i documenti per, ad esempio, la verifica giudiziaria in caso di contenzioso.

Upload di un nuovo documento

L'upload di un nuovo documento avviene utilizzando il web service DocumentService (con username/password codificata e valorizzata nell'header SOAP).
In caso di mancanza di tale informazione, la chiamata al web service andrà in errore.
Il complex-type UploadResponse, ritornato dal web service è costituito come segue:

Campo	Tipo	Descrizione
Status	String	Esito chiamata; valorizzato con "OK" in caso di esito positivo o con un codice di errore
Mida	String	Codice MIDA del nuovo documento caricato (valorizzato solo se Statu OK)
ErrorMessage	String	Messaggio di errore ritornato da web service (calorizzato solo se Status OK)

16 LA GESTIONE DEL CONTENZIOSO

Il processo di gestione di un contenzioso, inizialmente segue le classiche politiche di gestione previste dalla SGR ma, qualora vi sia un ordine dell'Autorità Giudiziaria in tal senso, sarà necessario procedere ad una perizia dei dati informatici delle firme in contenzioso.

Per questo motivo Xyzmo mette a disposizione un software che permette la visione dei dati informatici e delle modalità di generazione della firma a mezzo di una ricostruzione utilizzando i parametri memorizzati.

Ovviamente per poter effettuare questo controllo è indispensabile poter accedere ai dati crittografati della firma.

In sintesi il processo prevede:

a) L'Autorità Giudiziaria impartisce l'ordine al soggetto incaricato della perizia;

b) L'Autorità Giudiziaria definisce la sede dove si svolgerà la perizia (tribunale; ufficio del perito; sede della Certification Authority o altra sede) ed i tempi di effettuazione della perizia;

c) Viene richiesto, alla società di conservazione, l'originale elettronico del documento;

d) Nella sede individuata, la Certification Authority (o la/le risorse indicate come referenti) inseriscono la Password per permettere di accedere alla chiave di decriptazione che sarà utilizzata nel sistema di perizia fornito da Xyzmo;

e) Il perito rileva i dati informatici per verificare se questi siano congruenti con la modalità di generazione della firma del documento.

Manuale Operativo

Manuale Operativo

Firma Elettronica Avanzata FEA

Firma con Token

Azimut Financial Insurance S.p.A.

Data	1 Ottobre 2016
Versione	1.0
Stato	Definitivo

1 SOMMARIO

2 PREMESSA

Il presente documento riporta le informazioni relative al progetto di Firma Elettronica Avanzata con Token che ha realizzato il Gruppo Azimut. Il progetto di Firma Elettronica Avanzata è stato realizzato per la società del Gruppo Azimut: Azimut Financial Insurance S.p.A.

3 DEFINIZIONI

3.1 DEFINIZIONI RIGUARDANTI I SOGGETTI

Soggetto	Illustrazione
Certificatore	È l'ente, pubblico o privato, abilitato a rilasciare certificati digitali previa specifica procedura di certificazione in conformità con gli standard nazionali ed europei.
Addetto all'attività di intermediazione	È la persona incaricata, dal Soggetto che eroga i servizi di Firma Elettronica Avanzata, all'identificazione del Cliente; lo informa in merito alle condizioni d'uso e alle modalità del servizio; partecipa al processo di attivazione della Firma Elettronica Avanzata da parte dell'utente.
Soggetti erogatori dei servizi di Firma Elettronica Avanzata	Sono i soggetti giuridici che erogano soluzioni di Firma Elettronica Avanzata al fine di utilizzarle nei rapporti intrattenuti con soggetti terzi per motivi istituzionali, societari o commerciali, realizzandole in proprio o anche avvalendosi di soluzioni realizzate dai soggetti che le realizzano come attività di impresa.
Soggetti realizzatori dei servizi di Firma Elettronica Avanzata	Sono i soggetti giuridici che, quale oggetto dell'attività di impresa, realizzano soluzioni di Firma Elettronica Avanzata a favore di Soggetti erogatori.
Titolare	E' la persona fisica identificata dal Certificatore, cui è stata attribuita la firma digitale (o remota) ed è stata consegnata la chiave privata del certificatore stesso.
Cliente	È il soggetto a favore del quale la licenziataria mette a disposizione una soluzione di Firma Elettronica Avanzata al fine di sottoscrivere i documenti informatici.

3.2 ACRONIMI, DEFINIZIONI E TERMINI UTILIZZATI

Sigle	Illustrazione
AES	Acronimo di Advanced Encryption Standard è un algoritmo (utilizzato come standard dal governo degli Stati Uniti) di cifratura a blocchi e a chiave simmetrica operante su un gruppo di bit a lunghezza finita.
AgID	Agenzia per l'Italia Digitale (come da Decreto Legislativo 22 giugno 2012 n.83 articolo 22) ha sostituito CNIPA e DigitPa.
CAD	Il codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n.82 e successivi modificazioni.
Certificato digitale	Nella crittografia asimmetrica un certificato digitale è un documento elettronico che attesta l'associazione univoca tra una chiave pubblica e l'identità di un soggetto (una persona, una società, un computer, etc) che dichiara di utilizzarla nell'ambito delle procedure di cifratura asimmetrica e/o autenticazione tramite firma digitale.
Certificato qualificato	Il certificato digitale conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II del medesima direttiva.
Chiave Privata	È la chiave di crittografia utilizzata in un sistema di crittografia asimmetrica al fine di proteggere la firma apposta. La chiave privata è associata a una chiave pubblica ed è in possesso del Titolare che la utilizza per firmare digitalmente i propri documenti.
Chiave Pubblica	E' la chiave crittografica in un sistema di crittografia asimmetrica ed è utilizzata per verificare la firma digitale apposta su un documento informatico dal titolare della chiave asimmetrica. Tale chiave è associata ad una chiave Privata.
CNIPA (DigitPA)	Centro Nazionale per l'Informatica nella Pubblica Amministrazione. E' l'organismo di controllo istituito dal Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri.
Dispositivo sicuro per creazione della Firma	Dispositivo Hardware in grado di proteggere in modo efficace la segretezza della chiave privata.
Dispositivi sicuri per la generazione della Firma Elettronica	Mezzi sui quali il firmatario può conservare un controllo esclusivo la cui conformità è accertata ai sensi dell'art. 12 del DPCM 22/02/2013
Dispositivi sicuri per la generazione della firma Digitale	Mezzi sui quali il firmatario può conservare un controllo esclusivo la cui conformità è accertata ai sensi dell'art. 13 del DPCM 22/02/2013
Documento Informatico	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Sigle	Illustrazione
Documento analogico	La rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.
Duplicato informatico	Documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo su dispositivi diversi, della medesima sequenza di valori binari del documento originario.
Copia informatica di documento informatico	Il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza dei valori binari
Firma Elettronica	L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.
Firma Elettronica Avanzata (FEA)	Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.
Firma Elettronica Qualificata	Un particolare tipo di Firma Elettronica Avanzata che sia basata su un certificato qualificato e realizzata tramite un dispositivo sicuro per la creazione ella firma.
Firma digitale	Particolare tipo di Firma Elettronica basata su un certificato qualificato e su un sistema di chiavi crittografiche, pubblica e privata, correlate tra loro, consentendo al titolare, tramite chiave privata, e al destinatario, tramite chiave pubblica, di rendere manifesta e di verificare la provenienza e l'integrità di uno o un insieme di documenti informatici.
Gestione informatica di documenti	L'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato, effettuato mediante sistemi informatici.
HASH	Funzione matematica che genera, a partire da un'evidenza informatica, un'impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
Marca Temporale (Timestamp)	Riferimento temporale che consente la validazione temporale (data certa) e che dimostra l'esistenza di un'evidenza informatica in un tempo certo.
PAdes	Formato di busta crittografica definito nella norma ETSI TS 102 778 basata a sua volta sullo standard ISO/IEC 32000 e successive modifiche.

Sigle	Illustrazione
PDF	È uno standard aperto per lo scambio di documenti elettronici incluso nella categoria ISO (International Organization for Standardization).
RSA	Algoritmo di crittografia asimmetrica. Questo algoritmo si basa su utilizzo di chiavi pubblica e privata.
SHA-1	Acronimo di Secure Hash Algorithm: identifica un algoritmo che genera un'impronta digitale di 160 bit.
SHA-256	Acronimo di Secure Hash Algorithm: identifica un algoritmo che genera un'impronta digitale di 256 bit.
SHA-512	Acronimo di Secure Hash Algorithm: identifica un algoritmo che genera un'impronta digitale di 512 bit.
Token	E' il PIN CODE inviato all'utente tramite SMS. Il PIN CODE ha valenza temporanea e può essere usato una sola volta. Ogni PIN CODE è associato ad un solo Transaction ID che identifica la richiesta di firma per la quale è stato inviato il PIN CODE
Timbro di Firma	Contiene il Nome e Cognome dell'utente che ha firmato, il Token utilizzato per firmare, il Transaction ID dell'operazione di firma associata al Token
Blob di Firma	Contiene il codice NDG dell'utente che ha firmato, il Nome e Cognome dell'utente che ha firmato, il numero di telefono associato al TOKEN utilizzato per firmare, la data di firma
Soluzioni di Firma Elettronica Avanzata	Soluzioni strumentali alla generazione e alla verifica della Firma Elettronica Avanzata di cui all'art. 1, comma 1, lettera q-bis del CAD

RIFERIMENTI NORMATIVI

Item	Riferimenti	Descrizioni
(0)	**1999/93/CE**	Direttiva del Parlamento Europeo e del Consiglio del 13 dicembre 1999 relativa a una comune visione comunitaria in tema di firme elettroniche.
(1)	**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.
(2)	**D.Lgs. 196/2003**	Decreto Legislativo 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali".
(3)	**D.Lgs. 82/2005**	Decreto Legislativo 7 marzo 2005 N. 82 "Codice dell'amministrazione Digitale".
(4)	**D.Lgs. 4 aprile 2006 n. 159**	Decreto Legislativo 4 aprile 2006 N. 159.Disposizione integrative e correttive al decreto legislativo 7 marzo 2005, n.82, recante codice dell'amministrazione digitale.
(5)	**DPCM 12 ottobre 2007**	Decreto del Presidente del Consiglio dei Ministri 12 ottobre 2007. Differimento del termine che autorizza l'autodichiarazione circa a rispondenza ai requisiti di sicurezza a cui all'art. 13, comma4, del DPCM, pubblicato sulla Gazzetta Ufficiale del 30 ottobre 2003, n. 13.
(6)	**DPCM 30 marzo 2009**	Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009. Il presente decreto abroga il DCPM del 13 gennaio 2004 "Regole Tecniche" in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici. (Gazzetta Ufficiale n. 129 del 6 giugno 2009).
(7)	**D.Lgs. 235/2010**	Decreto Legislativo 30 dicembre 2010 n. 235. Modifiche ed integrazioni al D.Lgs. 7 marzo 2005 n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge n. 69 del 18 giugno 2009. Codice dell'amministrazione digitale pubblicato su Gazzetta Ufficiale n. 6 del 10 gennaio 2011.
(8)	**D.Lgs. n.83 22 giugno 2012**	Decreto Legislativo n. 83 del 22 giugno 2012 Art 22 Sospensione di CNIPA e DigitPA che confluiscono nell'**Ag**enzia per l'**I**talia **D**igitale (AgID).

Item	Riferimenti	Descrizioni
(9)	**D.Lgs. N. 221 17 dicembre 2012**	Decreto Legislativo n. 221 del 17 dicembre 2012 “Misure Urgenti per la crescita del Paese”. Il CAD, modificato nell’articolo 21, afferma il principio secondo cui “l’utilizzo del dispositivo di Firma Elettronica Qualificata o Digitale si presume riconducibile al titolare, salvo che questi dia prova contraria”. (la FEA è riportata ai metodi di disconoscimento classici del codice di procedura civile Art 214).
(10)	**Regole Tecniche DPCM 22 febbraio 2013**	Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013 “Regole Tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3,24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, 3 e 71.
(11)	**Regolamento UE n. 910/2014**	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

4 GLI ATTORI

4.1 SOGGETTO CHE EROGA LA SOLUZIONE

Azimut Financial Insurance S.p.A., come da articolo 55 comma 2 lettera a) del Decreto del Presidente del Consiglio dei Ministri datato 22 febbraio 2013, si identifica come Soggetto che eroga la soluzione di Firma Elettronica Avanzata, con Token, al fine di utilizzarla nei rapporti intrattenuti con soggetti terzi (utenti o clienti) per motivi commerciali.

4.1.1 DATI IDENTIFICATIVI

Ragione Sociale	**Azimut Financial Insurance S.p.A.**
Indirizzo sede	Via Cusani 4 – 20121 Milano
Legale Rappresentante	Pietro Giuliani
Codice Fiscale	09105230966
Partita IVA	09105230966
Registro Imprese	Milano
REA	2068907
Capitale Sociale (in Euro)	50.000,00 i.v.
Indirizzo E-Mail	info@azimut.it
Numero Telefonico	02 8898 1
Numero FAX	02 88985500
Indirizzo Sito istituzionale	www.azimut.it

4.1.2 ASSISTENZA CLIENTE

Per contattare Azimut Financial Insurance S.p.A. al fine di ricevere informazioni ed assistenza sul servizio di FEA il cliente può:

- Contattare AFI all'indirizzo postale **Azimut Financial Insurance S.p.A. Via Cusani 4 20121 Milano;**

- Contattare Addetto all'attività di intermediazione di riferimento;
- Chiamare il numero Assistenza Clienti MyAzimut indicato sulla brochure informativa pubblicata sul sito internet di Azimut.

4.2 SOGGETTO CHE REALIZZA LA SOLUZIONE DI FIRMA ELETTRONICA AVANZATA CON TOKEN

In aderenza a quanto espresso nell'Art, 55 comma 2 lettera b) del DCPM datato 22.2.2013, si segnala che il software di Firma Elettronica Avanzata con Token utilizzata da Azimut Financial Insurance S.p.A. è stata realizzata dalla società XYZMO Software GmbH con sede ad Ansfelden in Austria, la soluzione è denominata Click to Sign. XYZMO Software GmbH opera da oltre 10 anni nei sistemi di Firma Elettronica Avanzata.

4.3 ALTRE SOGGETTI COINVOLTI

4.3.1 STUDIO LEGALE ZITIELLO E ASSOCIATI

Studio legale che ha curato la consulenza legale per la **AFI**.

4.3.2 OBJECTWAY FINANCIAL SOFTWARE SPA

Società che realizza la piattaforma di collocamento e di distribuzione di prodotti e contratti di assicurazione di prodotti e servizi bancari integrando il software di Firma con Token Click to Sign e conserva presso il proprio Data Center i server XYZMO acquistati dalla **AFI** ma dei quali cura installazione, gestione e aggiornamento.

4.3.3 POSTEL SPA

Cura l'attività di archiviazione, apposizione della data certa e conservazione a norma dei documenti digitali sottoscritti con FEA.

4.3.4 ACTALIS SPA

In qualità di Certification Authority fornisce il certificato asimmetrico di crittografia, il certificato non qualificato di firma e la loro installazione. Conserva inoltre le chiavi private di cifratura del certificato utilizzato per crittografare le firme poste sui documenti.

5 SCOPO DEL DOCUMENTO

Questo documento ha lo scopo di descrivere le caratteristiche, le modalità operative, le procedure adottate e le regole predisposte ed utilizzate dagli operatori incaricati dalla **AFI** e dai Clienti della **AFI** al fine di gestire i servizi di Firma Elettronica Avanzata con Token. Il documento recepisce quanto richiesto dalle Regole Tecniche del 22 febbraio 2013.

In particolare sono descritte, nel documento, le procedure atte a soddisfare quanto richiesto in tema di generazione, apposizione e verifica della Firma Elettronica Avanzata, Firma Digitale Remota e Validazione Temporale dei documenti informatici. Sono recepite le indicazioni espresse dal **CAD** e successive modifiche riportate nel D.Lgs. del 30 dicembre 2010, n. 235 e dal DCPM 22 febbraio 2013 (di seguito, le "**Regole Tecniche**").

La **AFI** provvederà annualmente alla verifica della conformità della propria soluzione di Firma Elettronica Avanzata e, ove si renderà necessario, provvederà ad aggiornare questo documento anche in considerazione dell'evoluzione della normativa e degli standard tecnologici.

6 FINALITÀ

Con il progetto di Firma Elettronica Avanzata con Token, la **AFI** intende far sottoscrivere ai clienti interessati in formato digitale moduli, contratti, disposizioni e altri documenti relativi ai prodotti e servizi forniti dalla AFI e dalle società terze con cui ha stipulato apposite convenzioni. Firmare documenti direttamente in formato elettronico utilizzando la Firma Elettronica Avanzata permetterà alla **AFI** di poter digitalizzare i processi cartacei ai fini di una maggiore efficienza, un miglior servizio alla propria clientela ed un maggior rispetto per l'ambiente.

7 QUADRO NORMATIVO

Il processo di **FEA** realizzato rispecchia quanto espresso nella normativa in essere con particolare riferimento al **CAD**.

Sul piano probatorio, l'art. 21, comma 2 del CAD precisa infatti che il documento informatico sottoscritto con firma elettronica avanzata (ma anche qualificata o digitale) – che garantisce determinati requisiti – ha l'efficacia prevista dall'art. 2702 c.c., ossia di scrittura privata.

Inoltre, la nuova formulazione dell'art. 21, comma 2-bis, del CAD recita: "*Salvo quanto previsto dall'articolo 25, le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma*

digitale. Gli atti di cui all'articolo 1350, numero 13) del codice civile soddisfano comunque il requisito della forma scritta se sottoscritti con firma elettronica avanzata, qualificata o digitale".

Il requisito della forma scritta è previsto, a pena di nullità, per i contratti relativi ai servizi di investimento ai sensi dell'art. 23 del d.lgs. 24 febbraio 1998, n. 58 (di seguito "**TUF**").

Il quadro normativo di riferimento è individuabile nelle Regole Tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali.

8 FIRMA CON TOKEN COME FIRMA ELETTRONICA AVANZATA

Per poter essere valida come FEA, la Firma con Token deve garantire il rispetto dei requisiti previsti dall'art. 56 delle Regole Tecniche.

In particolare e a tal fine, la soluzione di firma scelta dalla AFI garantirà:

1) L'identificazione del firmatario del documento;
2) La connessione univoca della firma al firmatario;
3) Il controllo esclusivo del firmatario del sistema di generazione della firma
4) La possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma;
5) La possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;
6) L'individuazione del soggetto di cui all'articolo 55, comma 2, lettera (a) delle Regole Tecniche;
7) L'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificare gli atti, fatti o dati nello stesso rappresentati;
8) La connessione univoca della firma al documento sottoscritto;

Nello specifico, il processo disegnato per la **AFI** rispecchia i punti elencati e, di conseguenza, la Firma con Token adottata si configura come Firma Elettronica Avanzata

A tale fine, la **AFI** per rispondere positivamente a quanto richiesto, ha adotta le seguenti misure:

Identificazione del firmatario del documento	L'utente che intende firmare il documento si deve collegare alla sua area riservata MyAzimut tramite le credenziali personali che solo lui può conoscere e di cui è responsabile.
Connessione univoca della firma con il	L'utente può apporre la firma solo dove è previsto che sia lui a

firmatario	firmare. Il Token da utilizzare per la firma, ha una validità temporanea e viene inviato esclusivamente al numero di telefono che il cliente stesso ha comunicato in fase di sottoscrizione del Servizio Firma Elettronica Avanzata con Token o di cui ha richiesto una variazione in una fase successiva tramite apposito modulo di variazione dati contrattuali.
Controllo esclusivo del firmatario del sistema di generazione della firma	La firma apposta unisce 3 strumenti che sono sotto il diretto controllo del firmatario (numero di telefono su cui ricevere il Token, il Token temporaneo e l'accesso all'area riservata MyAzimut). Inoltre il firmatario può sempre: scorrere il documento; confermare la firma apposta; cancellare la firma apposta e ripetere la firma; annullare l'operazione di firma.
Possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma	L'integrità del documento è garantita dal processo che prevede l'apposizione di una firma informato PAdEs con contestuale generazione di Hash. Esiste sempre la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma. Presso il sito dell'Agenzia per l'Italia Digitale (URL http://www.agid.gov.it/identitadigitali/firme-elettroniche/software-verifica) sono disponibili gratuitamente software per la verifica dell'integrità del documento in conformità alla delibere CNIPA del 21 maggio 2009 num.45, è altresì possibile esigere la verifica con Adobe Acrobat Reader.
Possibilità per il firmatario di ottenere evidenza di quanto sottoscritto	Il firmatario ha la visione completa del documento sottoposto a firma e può scorrerlo per l'esamina. Oltre a ciò il processo prevede la consegna della copia de documento firmato ovvero con trasmissione elettronica o via email o con accesso ad un'area riservata sicura.
Individuazione del soggetto di cui all'art. 55, comma 2, lettera (a)	La **AFI** è identificabile come soggetto proponente e ha previsto tutto quanto necessario nel rispetto del requisiti previsti dall'art. 55 comma 2 lettera (a)
Assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificare gli atti, fatti o dati nello stesso rappresentati	Il documento generato nel processo di firma è nel formato PDF e chiuso con certificato riconducibile alla **AFI**.
Connessione univoca della firma al documento sottoscritto	Il processo previsto consente quanto richiesto attraverso la generazione di Hash al momento della firma, questi possono essere utilizzati poi in fase di verifica e controllo. La connessione univoca è garantita dalla soluzione adottata SIGNificant che utilizza algoritmi di cifratura collegate all'impronta del documento

9 OBBLIGHI

I soggetti che erogano soluzioni FEA (la **AFI**) hanno una serie di obblighi al fine di garantire il rispetto di tutti i requisiti richiesti dalla normativa di settore sopra menzionata. Tali requisiti sono riepilogati di seguito, mentre nei paragrafi successivi si illustrano dettagliatamente le modalità utilizzate dalla AFI per garantirne il rispetto.

1) Identificare in modo certo l'utente tramite un valido documento di riconoscimento;
2) Informare l'utente in relazione agli esatti termini e condizioni d'uso del servizio, compresa ogni eventuale limitazione d'uso;
3) Subordinare l'attivazione del servizio alla sottoscrizione di una dichiarazione di accettazione delle condizioni del servizio da parte dell'utente;
4) Conservare per almeno **20 anni** copia del documento di riconoscimento e la dichiarazione del punto 3;
5) Garantire la disponibilità, integrità, leggibilità e autenticità del documento di accettazione del servizio (punto 3);
6) Fornire liberamente e gratuitamente copia della dichiarazione e le informazioni di cui al punto 3) al firmatario su sua richiesta;
7) Rendere note le modalità con cui effettuare la richiesta di cui al punto 6), pubblicandole anche sul proprio sito internet;
8) Rendere note le caratteristiche del sistema realizzato atte a garantire quanto prescritto dalle Regole Tecniche articolo 56, comma 1;
9) Specificare le caratteristiche delle tecnologie utilizzate e come queste consentono di ottemperare a quanto prescritto;
10) Prevedere la possibilità di revoca del servizio da parte del cliente/utente.

9.1 IDENTIFICAZIONE DEL FIRMATARIO

L'identificazione del firmatario (Cliente) viene effettuata dagli operatori incaricati della **AFI** (Addetti all'attività di intermediazione) e, a tal fine, vengono richiesti documenti di identità e codice fiscale. Tutti i documenti debbono essere in corso di validità.

Per quanto concerne i documenti di riconoscimento, come da articolo 35 del DPR 445/2000, sono considerati validi i seguenti:

- ✓ Carta d'identità
- ✓ Passaporto
- ✓ Patente di Guida
- ✓ Patente Nautica
- ✓ Libretto della Pensione
- ✓ Patentino di abilitazione alla conduzione di impianti termici
- ✓ Porto d'Armi

In alternativa è possibile utilizzare altre tessere di riconoscimento purché presentino fotografia e timbri di validazione e siano rilasciate da una Amministrazione delle Stato.

Il codice fiscale può essere reperito da documenti rilasciati dall'Agenzia delle Entrate. Ad oggi risultano validi: Codice fiscale sia in forma cartacea o tesserino plastico; Tessera Sanitaria.

9.2 INFORMARE L'UTENTE FIRMATARIO

Gli Addetti all'attività di intermediazione, in qualifica di operatori della **AFI**, prima di procedere con la richiesta di accettazione dell'utilizzo del servizio FEA, procedono a informare il firmatario (Cliente) in relazione alla finalità (come espresso nel capitolo 6) le limitazioni d'uso (capitolo 7). Viene anche presentata e, se richiesta, consegnata, informativa dettagliata per l'utilizzo del servizio.

9.3 DICHIARAZIONE DI ACCETTAZIONE

Gli Addetti all'attività di intermediazione della **AFI** dopo aver adeguatamente informato il firmatario (Cliente), chiedono la sottoscrizione della dichiarazione di accettazione delle condizioni di erogazione del servizio da parte del cliente. Tale documento riporta tutti i dati informativi del cliente, la descrizione del servizio e richiede firme analogiche su documento cartaceo per l'accettazione del servizio e modifiche di rapporto.

9.4 CONSERVAZIONE DOCUMENTI RICHIESTI

In pieno rispetto di quanto previsto nell'articolo 56 comma 1 del DPCM 22/02/2013, al fine di dare evidenza di quanto previsto, si eseguono copia del documento di riconoscimento e del codice fiscale. Queste copie, in allegato al documento di accettazione del servizio, verranno conservate per almeno 20, anni dalla **AFI** garantendone, per tutto il periodo richiesto la disponibilità, integrità e leggibilità.

9.5 GARANZIA DI DISPONIBILITÀ, INTEGRITÀ E LEGGIBILITÀ DEL DOCUMENTO DI ACCETTAZIONE DEL SERVIZIO E MESSA A DISPOSIZIONE GRATUITA DEL DOCUMENTO DI ACCETTAZIONE

Su richiesta del firmatario (Cliente) effettuata mediante comunicazione scritta, la **AFI** si rende disponibile a fornire, senza oneri per il firmatario, copia cartacea della dichiarazione di accettazione da parte del Cliente stesso delle condizioni e dei termini del Servizio oltre alle copie dei documenti firmati con FEA e conservati in copia informatica al solo scopo di informazione.

Il Cliente potrà contattare l'Addetto all'attività di intermediazione di riferimento o direttamente la AFI per ricevere assistenza per attivare la richiesta.

9.6 CARATTERISTICHE DEL SISTEMA DI FIRMA

Al fine di ottemperare alla normativa di cui articolo 56 comma 1, la **AFI**, nel paragrafo 12 descrive le misure adottate a garanzie di quanto prescritto.

9.7 LA TECNOLOGIA UTILIZZATA

Nel paragrafo 13, la **AFI**, descrive in modo dettagliato le caratteristiche hardware e software al fine di ottemperare quanto richiesto dalle Regole Tecniche DPCM 22/02/2013.

9.8 PUBBLICAZIONE SUL SITO

La **AFI**, in ottemperanza a quanto richiesto dalla normativa in essere, ha pubblicato sul sito internet www.azimut.it il presente documento che descrive anche le caratteristiche del sistema di firma e le caratteristiche delle tecnologie utilizzate.

9.9 SERVIZIO DI REVOCA

Il processo di Firma Elettronica Avanzata adottato dalla **AFI** permette la revoca dei servizi tramite apposita richiesta scritta da parte del cliente. In caso di revoca la FEA non potrà più essere utilizzata.

Il cliente potrà contattare l'Addetto all'attività di intermediazione di riferimento o direttamente la AFI per ricevere assistenza per attivare le richiesta di Revoca.

10 TUTELA ASSICURATIVA

Ulteriore richiesta espressamente citata nelle Regole Tecniche, prevede una copertura assicurativa a garanzia del firmatario.

Il soggetto che eroga soluzioni di Firma Elettronica Avanzata si impegna a stipulare una polizza assicurativa per la copertura dei rischi dell'attività svolta e dei danni a tutela delle parti (Firmatari ed i Terzi) per almeno Euro 500.000,00(cinquecentomila/00).

La **AFI**, in qualità di soggetto che eroga la soluzione di Firma Elettronica Avanzata, ha stipulato polizza assicurativa con primaria compagnia Assicurativa per la copertura dei suddetti rischi.

11 LA SOLUZIONE AZIMUT

In tema di firma con Token, XYZMO ha prestato particolare attenzione alla sicurezza del dato di firma. Infatti, mentre il firmatario esegue la firma, i dati che caratterizzano la firma ovvero il Blob di Firma sono cifrati nella memoria del dispositivo mobile con la chiave simmetrica AES, la cui chiave a sua volta è cifrata con la chiave pubblica l'algoritmo asimmetrico RSA.

Il firmatario ha il controllo esclusivo del processo di firma disponendo di una serie di funzioni e può:

- Scorrere il documento senza limitazioni al fine di poter aver evidenza di quanto da lui sarà sottoscritto;
- Selezionare l'area di firma su cui vuole firmare
- Inserire nell'apposita area di firma selezionata il Token inviato tramite SMS;
- Modificare il Token inserito qualora si accorga di averlo inserito in maniera errata
- Richiedere nuovamente un nuovo Token qualora abbia cancellato per errore l'SMS inviato o qualora non sia arrivato l'SMS
- Annullare l'operazione di firma, qualora non voglia più firmare, con la selezione della funzione **ANNULLA**;
- Confermare la firma apposta con la selezione della funzione **OK**;
- Completare il processo di firma del documento con la selezione della funzione **CHIUDI**
- Annullare il processo di firma del documento qualora non sia più propenso a firmare, con la seleziona della funzione **CANCELLA**.

Con la conferma (funzione **OK**) da parte del firmatario alla firma apposta, il SIGNificant Client invia il Blob di Firma al SIGNificant Server che calcola l'impronta del documento con l'algoritmo SHA.

I dati cifrati, la chiave ASE cifrata, e l'impronta (HASH) del documento, sono inseriti nel documento PDF, alla fine del processo di firma del documento il SIGNificant Server firma il documento in standard PAdES, secondo la deliberazione CNIPA 21 maggio 2009, n.45.

Quest'ultima firma, garantisce l'integrità (documento non alterato) e autenticità (autore) del documento digitale (gruppo Azimut).

I dati così protetti non possono essere decriptati, visualizzati ed esaminati. Unica possibilità è di poter disporre della chiave privata, chiave in possesso solo di ente terzo e con regole di consegna solo per particolari eventi, e di un apposito software di analisi.

Questa operazione è prevista come processo di gestione di eventuali contenziosi.

11.1 IL SOFTWARE DI FIRMA

Per la realizzazione del servizio di Firma Elettronica Avanzata con Firma Token, **Azimut Financial Insurance S.p.A.** ha utilizzato un software denominato Click to Sign di Xyzmo il cui client è installato sulla postazione mobile e Web dei clienti della AFI.

La soluzione di Xyzmo mette a diposizione, per questo progetto, le componenti: SIGNificant Server; SIGNificant Client ed Identity Server.

11.2 IL SIGNIFICANT CLIENT

E' la componente inclusa nell' APP iOS ed Android installata sui dispositivi Mobile e sulla component Web presente nei PC del firmatario (Cliente) ed ha il compito di ricevere e visualizzare i documenti da sottoporre all'utente firmatario, di acquisire il Token temporaneo, di cifrarli insieme ad altre informazioni (chiave AES cifrata) e di inviarli al SIGNificant Server.

Il SIGNificant Client, per la cifratura delle informazioni, utilizza due differenti algoritmi di cifratura, un primo algoritmo di cifratura simmetrica AES-256 per cifrare i dati che caratterizzano la firma ovvero il Blob di Firma; un secondo algoritmo di cifratura asimmetrica RSA (chiave pubblica) per cifrare la chiave AES-256. La chiave AES-256 è generata in maniera casuale da SIGNificant Client per ogni firma. La chiave pubblica di cifratura utilizzata dall'algoritmo RSA è compilata insieme al SIGNificant Server e SIGNificant Client.

11.3 IL SIGNIFICANT SERVER

E' il server di gestione dell'attività di firma, installato presso ObjectWay, riceve il documento in formato PDF dal SIGNificant Client, lo trasforma in immagine ottimizzata e lo invia al SIGNificant Client.

Il SIGNificant Client dopo aver acquisito i dati che caratterizzano la firma li invia cifrati al SIGNificant Server**,** il SIGNificant Server verifica la corrispondenza, inserisce il Blob di Firma del firmatario e la chiave AES cifrata nel documento ed invia al SIGNificant Client l'esito positivo dell'inserimento della firma.

Con la conferma da parte del SIGNificant Client della conclusione delle operazioni di firma il SIGNificant Server rende il documento non modificabile grazie all'apposizione di certificato di chiusura, rilasciata da una Certification Authority accreditata presso AgID.

Il SIGNificat Server utilizza l'algoritmo di cifratura simmetrica SHA-512 per calcolare l'impronta del documento informatico e l'algoritmo RSA per firmare digitalmente i documenti.

11.4 L'IDENTITY SERVER

E' il server che conserva l'associazione Utente e Numero di Cellulare cui inviare via SMS il Token per la firma.

L'Identity Server, dopo avere ricevuto dal SIGNificant Client la richiesta di firma del firmatario, verifica se il firmatario ha un numero di telefono associato, genera il Transaction ID di firma con il Token per firmare e invia il Token al numero di telefono associato al firmatario.

Dopo che il firmatario ha selezionato la funzione OK sulla maschera di firma, l'Identity Server verifica che il Token inserito dal firmatario nel punto firma sia corrispondente con il Transaction ID assegnato.

11.5 MODALITÀ DI FIRMA

La soluzione adottata si basa sulla tecnologia Xyzmo e su una architettura che prevede l'installazione di una specifica APP sui dispositivi Mobile disponibile sugli Store Apple ed Android e una applicazione WEB rivolta ai clienti del gruppo AZIMUT. Tali applicazioni permettono l'utilizzo della logica del SIGNificant Client di Xyzmo che comunica, solo in modalità On-Line e su canale sicuro HTTPS, con il SIGNificant Server di Xyzmo e l'Identity Server.

La prima attività che viene richiesta al cliente, in modo che possa poi usufruire del servizio di Firma Elettronica Avanzata con Token, è l'accettazione e sottoscrizione del consenso all'utilizzo della FEA. Tale consenso viene raccolto dall' Addetto all'attività di intermediazione dopo aver fatto leggere, illustrato e consegnato l'informativa al cliente.

Per la sottoscrizione di documenti digitali da parte dei clienti, è necessario che gli stessi abbiano inserito le proprie credenziali d'accesso alle applicazioni App o Web, e devono essere stati riconosciuti dal sistema informativo MyAzimut della AFI.

Al firmatario (Cliente) sono sottoposti documenti digitali in formato PDF con uno o più campi firma; il campo firma viene presentato al firmatario in modalità esplicita sulle applicazioni e l'intero foglio del documento è disponibile e visualizzato sullo stesso.

Il Firmatario firma grazie all'inserimento del Token inviato tramite SMS, l'utente mantiene il controllo esclusivo dell'operazione di firma, premendo il tasto OK accetta l'invio dei dati crittografati che verranno poi inseriti sul documento opportunamente protetto.

I dati sono acquisiti dal SIGNificant Client, cifrati, ed inviati al SIGNificant Server su un canale sicuro (HTTPS) che li inserisce nel documento.

A conclusione del processo di firma viene richiesta una conferma alla chiusura del documento con conferma delle firme. In caso di conferma il documento viene chiuso con un certificato non qualificato di chiusura a nome dell'azienda. Il documento chiuso con il certificato di chiusura viene poi messo a

disposizione del servizio di archiviazione e conservazione a norma fornito da Postel. In caso di non conferma, il documento viene cancellato dalla memoria del sistema operazioni di riscrittura su cache da parte dell'applicazione.

11.6 LA SICUREZZA

In tema di firma con Token, XYZMO ha prestato particolare attenzione alla sicurezza del dato di firma. Infatti, mentre il firmatario esegue la firma, i dati che caratterizzano la firma ovvero Il Blob di Firma sono cifrati con la chiave simmetrica AES, la cui chiave a sua volta è cifrata con la chiave pubblica l'algoritmo asimmetrico RSA.

Il firmatario ha il controllo esclusivo del processo di firma disponendo di una serie di funzioni e può:

- Scorrere il documento senza limitazioni al fine di poter aver evidenza di quanto da lui sarà sottoscritto;
- Selezionare l'area di firma su cui vuole firmare
- Inserire nell'apposita area di firma selezionata il Token inviato tramite SMS;
- Modificare il Token inserito qualora si accorga di averlo inserito in maniera errata
- Richiedere nuovamente un nuovo Token qualora abbia cancellato per errore l'SMS inviato o qualora non gli sia arrivato l'SMS
- Annullare l'operazione di firma, qualora non voglia più firmare, con la selezione della funzione **ANNULLA**;
- Confermare la firma apposta con la selezione della funzione **OK**;
- Completare il processo di firma del documento con la selezione della funzione **CHIUDI**
- Annullare il processo di firma del documento non sia più propenso a firmare, con la seleziona della funzione **CANCELLA**.

Con la conferma (funzione **OK**) da parte del firmatario alla firma apposta il SIGNificant Client invia i dati al SIGNificant Server che calcola l'impronta del documento con l'algoritmo SHA.

I dati cifrati, la chiave ASE cifrata, e l'impronta (HASH) del documento, sono inseriti nel documento PDF, alla fine del processo di firma del documento il SIGNificant Server firma il documento in standard PAdES, secondo la deliberazione CNIPA 21 maggio 2009, n.45.

Quest'ultima firma, garantisce l'integrità (documento non alterato) e autenticità (autore) del documento digitale (gruppo Azimut).

I dati così protetti non possono essere decriptati, visualizzati ed esaminati. Unica possibilità è di poter disporre della chiave privata, chiave in possesso solo di ente terzo e con regole di consegna solo per particolari eventi, e di un apposito software di analisi.

Questa operazione è prevista come processo di gestione di eventuali contenziosi.

11.7 INTEGRITÀ DEL DOCUMENTO SOTTOSCRITTO

L'integrità del documento sottoscritto dall'utente è garantita dal certificato riconducibile alla AFI opposto in chiusura di documento.

L'apposizione della firma elettronica è gestita dal SIGNificant Server.

Il SIGNificant Server al termine dell'inserimento dei dati di firma cifrati nel documento, calcola l'impronta con la chiave privata del certificato non qualificato, cifra l'impronta e la inserisce nel documento. Il risultato del processo è la firma del documento che ne garantisce l'integrità e autenticità.

La verifica dell'integrità ed autenticità del documento può essere svolta da un qualsiasi software di verifica conforme al CAD; ad esempio ADOBE ACROBAT READER.

La verifica dell'autenticità della sottoscrizione (la firma) dell'utente può essere eseguita solo quando si è in possesso della chiave privata di cifratura.

La chiave privata di cifratura è conservata presso un ente terzo fidato, **Actalis** in questo caso, che renderà disponibile la chiave solo su motivata (es. l'autorità giudiziaria) richiesta del legale rappresentante.

12 PROCESSO DI IDENTIFICAZIONE E FIRMA

Quando l'Addetto all'attività di intermediazione richiede al Cliente di apporre una o più firme con Token, può verificare se il Cliente ha già sottoscritto la dichiarazione di accettazione (come da paragrafo 10.3). Se risulta che il Cliente ha già sottoscritto la dichiarazione di accettazione, l'Addetto all'attività di intermediazione potrà procedere.

Se non risulterà che tale operazione sia stata sottoscritta ma il Cliente dichiara di averlo fatto (l'avvenuta sottoscrizione sarà disponibile su sistema dopo i controlli del back office) non si potrà procedere che con forma cartacea sino a che la verifica del back office non sia conclusa.

In ipotesi che non sia mai stata presentata la soluzione e, di conseguenza, mai sottoscritta, l'Addetto all'attività di intermediazione provvede ad informare in modo chiaro e completo il sottoscrittore come indicato nei paragrafi 10.2 e 10.3 e riportati nel modulo di accettazione. Richiederà i documenti previsti per l'attivazione del servizio di FEA con Token (come illustrato nel paragrafo 10.1), richiederà al cliente la sottoscrizione autografa della dichiarazione di accettazione come descritto nel paragrafo 10.3 e, successivamente, provvederà all'inoltro al back office dei documenti per la loro conservazione come da paragrafo 10.4.

L'utente potrà procedere, dopo che il back office avrà registrato la sua accettazione, a firmare tutti documenti proposti dalla **AFI** su documenti informatici, avendo la stessa efficacia della forma scritta (paragrafo 7).

12.1 ACCETTAZIONE DEL CLIENTE DEL SERVIZIO DI FIRMA ELETTRONICA AVANZATA CON TOKEN

In questa fase, l'Addetto all'attività di intermediazione, provvede ad informare, dando piena disponibilità della documentazione prodotta dal gruppo Azimut, al processo di sottoscrizione con FEA con Token. E' in questa fase che, se il cliente conferma di voler utilizzare questa modalità di firma, l'Addetto all'attività di intermediazione acquisisce la sottoscrizione, **su modulo cartaceo**, del consenso del cliente all'utilizzo della FEA e delle copie dei documenti da allegare.

I dati di:

- Numero di Telefono su cui il Cliente riceve il Token con cui firmare
- E-mail su cui il Cliente riceve le comunicazioni di disponibilità dei documenti ai fini della firma nell'area riservata (Area Firma) presente su MyAzimut

sono riportate all'interno dello stesso modulo cartaceo (Contratto Unico dei Servizi Digitali) che il Cliente sottoscrive per l'adesione al servizio di Firma Elettronica Avanzata di tipo Token. Ogni variazione degli stessi può avvenire solo attraverso la sottoscrizione di un modulo cartaceo di modifica dati contrattuale da parte

del Cliente, reso disponibile dalla AFI nella piattaforma MyAzimut; modulo che successivamente dovrà pervenire alla strutture di back-office per le opportune verifiche prima di recepire la richiesta di modifica.

12.2 IL PROCESSO DI FIRMA

I SIGNificant Client, SIGNificant Server e l'Identity Server sono in grado di firmare documenti in formato PDF con Firma Elettronica Avanzata con Token, ciò garantisce che un qualsiasi documento che può essere stampato può anche essere firmato.

Il processo di firma può essere sinteticamente descritto come segue:

- L'Addetto all'attività di intermediazione, tramite Web o il dispositivo mobile, si identifica al sistema MyDesk della AFI ed esegue l'accesso al sistema informativo del Gruppo Azimut con le proprie credenziali;
- L'Addetto all'attività di intermediazione compila ed invia in Area Firma condivisa con il Cliente il documento che desidera far sottoscrive al cliente;
- Il cliente, tramite Web o il dispositivo mobile, si identifica al sistema MyAzimut della AFI ed esegue l'accesso al sistema informativo del Gruppo Azimut con le proprie credenziali
- Il cliente accede alla propria Area Firma presente su MyAzimut e seleziona il documento che intende sottoscrivere
- Il documento PDF selezionato dal cliente viene inviato al SIGNificant Server;
- Il SIGNificant Server calcola l'impronta (HASH) del documento, ed invia al SIGNificant Client l'immagine PDF ottimizzata del documento;
- Il documento è visualizzato sul web o sul dispositivo mobile del cliente che attiva il processo di firma.

Il Cliente o sottoscrittore ha il controllo esclusivo del processo di firma e dispone delle seguenti funzioni:

- Visualizzazione del documento in modo da aver evidenza di quanto da lui sarà sottoscritto;
- Inserimento del Token nell'apposita area di firma;
- (**OK**) per confermare l'inserimento;
- (**ANNULLA**) per non procedere con l'inserimento del Token;
- (**CHIUDI**) per completare la firma del documento

- (**CANCELLA**) per annullare la firma del documento.

Mentre il sottoscrittore esegue la firma, i dati che caratterizzano la stessa sono cifrati con la chiave simmetrica AES, la cui chiave a sua volta è cifrata con la chiave pubblica l'algoritmo RSA (a chiavi asimmetriche).

Con la conferma (**OK**) da parte del firmatario il SIGNificant Client invia al SIGNificant Server, i dati della firma cifrati (Blob di Firma), la chiave AES cifrata. Il SIGNificant Server:

- Inserisce i dati ricevuti dal SIGNificant Client nel documento PDF originale residente sul server;
- Invia al SIGNificant Client l'immagine PFD ottimizzata del documento, con il Timbro di firma in bella vista.
- Il SIGNificant Client al ricevimento dell'immagine PDF ottimizzata se i sottoscrittori sono più di uno, o sono richieste più firme dello stesso soggetto, ripeterà le operazioni sopra descritte per un numero di volte necessarie.
- Il SIGNificant Client inoltra la conclusione della sottoscrizione del documento da parte dell'utente al SIGNificant Server.
- Il SIGNificant Server calcola l'impronta (HASH), cifra l'impronta e la inserisce nel documento. Il risultato del processo è la firma in formato PAdES del documento che ne garantisce l'integrità ed autenticità.
- Il SIGNificant Server invia al SIGNificant Client l'immagine PDF ottimizzata del documento firmato digitalmente.
- Il SiGNificant Server chiude il documento con un certificato non qualificato intestato alla società ovvero richiede la firma digitale remota per la chiusura del documento.
- Successivamente vengono chiamati opportuni Web Service per inviare il documento al servizio di archiviazione e conservazione a norma. Tale invio avviene a mezzo di web service, con trasmissione in sicurezza via https, a Postel ente di archiviazione e conservazione a norma. La chiamata via Web Service prevede il passaggio del documento firmato (criptato e chiuso con certificato aziendale) ed una serie di metadati per il controllo del documento. La Web Service ritornerà un esito che potrà essere OK (documento ricevuto correttamente, non corrotto e con tutti i metadati significativi presenti, validati e archiviato da Postel) e un codice MIDA contenente anche il riferimento del documento archiviato; ovvero riceverà un esito KO in presenza di documento corrotto, non conforme o mancanza di corrispondenza nei metadati. In caso di esito KO il documento viene cancellato e l'operazione deve essere ripetuta dall'inizio. L'operazione di inoltro è stimata in 10 millisecondi.

Successivamente vengono rese disponibili le copie elettroniche immagine del documento firmato al cliente,

all' Addetto all'attività di intermediazione ed al backoffice (o via WebService o in area riservata sicura chiamata Documenti).

12.3 LE COMUNICAZIONI CIFRATE

La comunicazione ed il trasferimento dei dati di firma tra il Client ed il Server sono su un canale HTTPS (criptato) con algoritmo asimmetrico. Questo protocollo, largamente utilizzato dai sistemi WEB, rende impossibile l'intercettazione dei contenuti in quanto si crea un canale di comunicazione criptato tra Client e Server attraverso lo scambio di certificati, una volta stabilita la connessione al suo interno è utilizzato il protocollo HTTP per l'invio e la ricezione dei dati.

Anche la comunicazione per l'invio del documento ottimizzato ed il trasferimento dei dati di firma tra il Client ed il Server sono su un canale HTTPS (criptato) con algoritmo asimmetrico.

13 ALTRI COMPONENTI

Per la realizzazione di un processo di firma in piena conformità con le Regole Tecniche emesse il 22/02/2013 con Decreto del Presidente del Consiglio dei Ministri, sono necessari i componenti obbligatori alcuni e opzionali altri, di seguito descritti.

13.1 CHIAVE PUBBLICA DI CIFRATURA

I dati di firma sono cifrati utilizzando una chiave asimmetrica generata dal software di firma, questa chiave è cifrata con chiave pubblica di cifratura. La chiave pubblica è compilata da XYZMO insieme al programma SIGNificant Cliente e sono generate da Actalis SPA in qualità di Certification Authority accreditata presso AgDI.

13.2 CHIAVE PRIVATA DI CIFRATURA

La chiave privata, unica in grado di estrarre in chiaro i dati di firma è generata da Actalis SPA in qualità di Certification Authority accreditata presso AgDI. Successivamente la chiave privata sarà conservata presso Actalis SPA in qualità di ente terzo. L'ente terzo sarà chiamato, in fase di eventuale contenzioso, dall'autorità giudiziaria seguendo il processo previsto per la gestione del contenzioso e illustrato in questo documento.

13.3 CERTIFICATO DI FIRMA

Il certificato di firma è installato sul SIGNificant Server ed è utilizzato al termine del processo di Firma Elettronica Avanzata, al fine di garantirne l'integrità (documento non alterato) ed autenticità del documento digitale.

13.4 MARCA TEMPORALE

Il software SIGNificant Server è in grado, qualora richiesto, di inserire nei documento sottoscritti digitalmente marche temporali (TIMESTAMP) conformi alla standard ISO 8601. La marca temporale è il risultato della procedura informatica con cui si attribuiscono, ai documenti informatici, una data ed un orario opponibili a terzi.

14 COMPONENTI DI SICUREZZA

14.1 SERVER

La soluzione applicativa e il software di Xyzmo sono installati su server dedicati ad **AZIMUT** gestiti nei Data Center di **Objectway** che garantiscono gli aspetti di disaster & recovery.

In relazione alle misure di sicurezza adottate il personale di **Objectway** dichiara che sono state messe in atto le misure minime richieste dall'allegato B del Codice Privacy.

In particolare i server non sono esposti all'esterno, la comunicazione è via https, gli accessi sono registrati su appositi log. **Objectway** ha predisposto apposito documento che illustra tutte le misure adottate recepito come allegato della Relazione Tecnica.

15 ARCHIVIAZIONE E CONSERVAZIONE A NORMA DEI DOCUMENTI

Il processo di archiviazione, apposizione della data certa e conservazione a norma è a carico di Postel che provvederà alla stesura del "Manuale di Conservazione" e assumerà la responsabilità della conservazione a norma per le sue componenti.

Per realizzazione di quanto previsto contrattualmente, Postel, mette a disposizione il sistema di archiviazione denominato "Documentum" ed il sistema "AOS" per l'archiviazione a norma.
Tutta l'operatività è posta in sicurezza e, di seguito, sono riassunte alcune caratteristiche tecniche.

Il sistema messo a disposizione da Postel è denominato GED Postel.

Il sistema GED prevede la seguente architettura fisica:

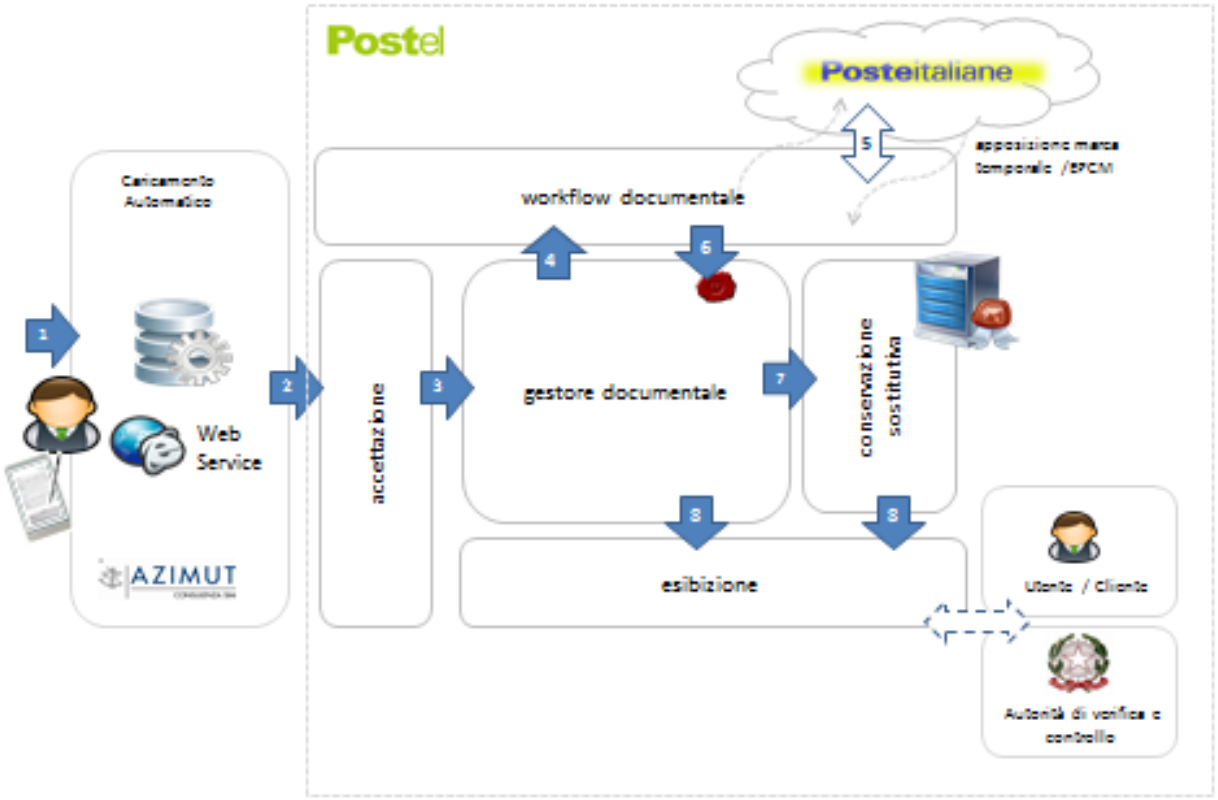
- Reverse Proxy IBM http Server 6.1, Apache web server (RP1),
- Data Server Oracle 10G in alta affidabilità (PB1, PB2),
- Content Serve con SO Red Hat Enterprise Linux 5.0 (CS1,CS2),
- Application Server con SO Red Hat Enterprise Linux 5.0 e Web Server IBM WS 6 (WS1, Ws2),
- Storage dati di tipo SAN (NAS (EMC DMX), EMC Centera,
- Client Acquisizione con SO Windows 2003 (OP1),
- Image Processing Component Server con SO Windows 2003 (IPCS1, IPCS2).

Il processo di archiviazione e conservazione dei documenti firmati è uno dei punti di attenzione del progetto. La regolamentazione per la protezione dei dati che presentano rischi specifici, come nel caso dei dati di firma elettronica avanzata, richiedono che i dati siano archiviati in sicurezza e in nessun punto del processo ci sia la possibilità di manipolazione dei dati. Per questo motivo, il gruppo Azimut, ha scelto di affidarsi a Postel.

Il processo delineato prevede che il documento firmato e chiuso con firma remota qualificata, venga inviato direttamente a Postel a mezzo di web service concordata. Postel marcherà temporalmente (con timestamp) il documento e ne creerà lotto per la conservazione a norma. Immagine del documento sarà disponibile su portale Postel agli utenti Azimut abilitati.

In sintesi il Processo si articola come di seguito:

- L'applicazione, dopo la chiusura del documento invoca una web service (via https) di Postel passando il documento sottoscritto, criptato e chiuso con un certificato intestato a Azimut Holding Spa. Oltre al documento vengono passati dei metadati che servono alla creazione degli indici del documento.
- L'applicazione di Postel esegue delle verifiche in merito alla congruenza dei metadati e di validità del documento ricevuto. Eseguito il controllo ritorna esito OK o KO a seconda dell'esito delle verifiche. Il codice MIDA di risposta, oltre all'esito, riporta anche la tipologia di errore ed identificativo del file per eventuali richiami del documento.
- Se la risposta è OK il documento viene archiviato nel sistema di archiviazione "Documentum" per poi procedere sino al processo di Archiviazione Ottica Sostitutiva a Norma.
- A timing prefissati il sistema documentale provvede a richiedere e marcare, con timestamp, ogni documento ricevuto, inoltrando poi tutti i documenti marcati al sistema di archiviazione e al sistema di Conservazione digitale a norma (AOS) .



Il sistema di archiviazione “Documentum” sarà la momentanea area di staging, prima di ottenere il TimeStamp (dalla CA) per poi passare immediatamente su sistema di Archiviazione a Norma (AOS) dove saranno conservati i file originari.

Gli operatori di Azimut (preventivamente segnalati e registrati, possono accedere al sistema di archiviazione per consultazione produzione di report statistici attraverso Il Portale Postel con l’accesso web denominato Taskspace. Esistono profilazioni diverse per le modalità di consultazione dei documenti (visore, base o supervisore).

L’utente “Visore”, con cui sono stati configurati gli user di Azimut, può soltanto consultare i documenti archiviati e conservati digitalmente, esibire a norma i documenti conservati e accedere alla reportistica.

I documenti originali presenti nel sistema di conservazione, possono essere richiesti in via ufficiale, utilizzando una richiesta formale e a mezzo di scritto, a Postel con firma di autorizzazione del Responsabile dell’archiviazione di Azimut e eventualmente dal rappresentante legale con motivazioni dichiarate e secondo un processo autorizzativo che sarà definito. Postel, su richiesta Azimut, produrrà un Dvd con i documenti per, ad esempio, la verifica giudiziaria in caso di contenzioso.

Upload di un nuovo documento

L'upload di un nuovo documento avviene utilizzando il web service DocumentService (con username/password codificata e valorizzata nell'header SOAP).
In caso di mancanza di tale informazione, la chiamata al web service andrà in errore.
Il complex-type UploadResponse, ritornato dal web service è costituito come segue:

Campo	Tipo	Descrizione
Status	String	Esito chiamata; valorizzato con "OK" in caso di esito positivo o con un codice di errore
Mida	String	Codice MIDA del nuovo documento caricato (valorizzato solo se Statu OK)
ErrorMessage	String	Messaggio di errore ritornato da web service (calorizzato solo se Status OK)

16 LA GESTIONE DEL CONTENZIOSO

Il processo di gestione di un contenzioso, inizialmente segue le classiche politiche di gestione previste dalla AFI ma, qualora vi sia un ordine dell'Autorità Giudiziaria in tal senso, sarà necessario procedere ad una perizia dei dati informatici delle firme in contenzioso.

Per questo motivo Xyzmo mette a disposizione un software che permette la visione dei dati informatici e delle modalità di generazione della firma a mezzo di una ricostruzione utilizzando i parametri memorizzati.

Ovviamente per poter effettuare questo controllo è indispensabile poter accedere ai dati crittografati della firma.

In sintesi il processo prevede:

a) L'Autorità Giudiziaria impartisce l'ordine al soggetto incaricato della perizia;

b) L'Autorità Giudiziaria definisce la sede dove si svolgerà la perizia (tribunale; ufficio del perito; sede della Certification Authority o altra sede) ed i tempi di effettuazione della perizia;

c) Viene richiesto, alla società di conservazione, l'originale elettronico del documento;

d) Nella sede individuata, la Certification Authority (o la/le risorse indicate come referenti) inseriscono la Password per permettere di accedere alla chiave di decriptazione che sarà utilizzata nel sistema di perizia fornito da Xyzmo;

e) Il perito rileva i dati informatici per verificare se questi siano congruenti con la modalità di generazione della firma del documento.