



Manuale Operativo

Manuale Operativo
Firma Elettronica Avanzata FEA
Firma Grafometrica
Azimut Capital Management SGR S.p.A.

Data	1 Ottobre 2016
Versione	1.3
Stato	Definitivo

1 SOMMARIO

1	Sommario	2
2	Premessa	5
3	Definizioni	6
3.1	Definizioni riguardanti i soggetti.....	6
3.2	Acronimi, definizioni e termini utilizzati	7
3.3	Riferimenti Normativi	10
4	Gli attori	12
4.1	Soggetto che eroga la soluzione	12
4.1.1	Dati Identificativi	12
4.1.2	Assistenza Cliente.....	12
4.2	Soggetto che realizza la soluzione di Firma Grafometrica.....	13
4.3	Altri soggetti coinvolti.....	13
4.3.1	Studio Legale Zitiello e Associati	13
4.3.2	Objectway Financial Software SPA.....	13
4.3.3	Magnetic Media Network SPA	13
4.3.4	Postel SPA.....	13
4.3.5	Actalis SPA.....	13
5	Scopo del Documento	15
6	Finalità.....	16
7	Quadro Normativo	16
8	Privacy.....	16
9	Firma grafometrica come firma elettronica avanzata	18
10	Obblighi	21
10.1	Identificazione del firmatario	22
10.2	Informare l'utente firmatario	22
10.3	Dichiarazione di accettazione.....	23

10.4	Conservazione documenti richiesti.....	23
10.5	Garanzia di disponibilità, integrità e leggibilità del documento di accettazione del servizio e messa a disposizione gratuita del documento di accettazione.....	23
10.6	Caratteristiche del sistema di firma.....	23
10.7	La tecnologia utilizzata	23
10.8	Pubblicazione sul sito	24
10.9	Servizio di revoca	24
11	Tutela assicurativa.....	24
12	La soluzione Azimut	25
12.1	Il Software di Firma.....	26
12.2	Il SIGNificant Client	26
12.3	Il SIGNificant Server	26
12.4	Modalità di firma	27
12.5	La sicurezza.....	28
12.6	Integrità del documento sottoscritto	29
13	Processo di Identificazione e firma	30
13.1	Deposito delle Firme Consulente.....	30
13.2	Deposito delle Firme Cliente	31
13.3	Il processo di firma	33
13.4	Le comunicazioni cifrate	34
14	Altri componenti	36
14.1	Chiave Pubblica di Cifratura.....	36
14.2	Chiave Privata di Cifratura	36
14.3	Certificato di firma.....	36
14.4	Marca Temporale	36
15	Componenti di sicurezza	37
15.1	Server.....	37
15.2	Device	37

16	Archiviazione e conservazione a norma dei documenti	39
17	La gestione del contenzioso	43

2 PREMESSA

Il presente documento riporta le informazioni relative al progetto di Firma Elettronica Avanzata con Firma Grafometrica 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 acquisizione 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 della 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.
Signature Tablet	Dispositivo elettronico che si connette ad un computer ed è in grado di acquisire dati biometrici comportamentali e grafici di una firma autografa. I valori acquisiti sono coordinate x-y; tempo; eventuale pressione.
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 DL 235/2010
Tablet	Dispositivo mobile (es. iPad) in grado di acquisire i dati biometrici di una firma autografa per mezzo di specifiche penne elettroniche.

3.3 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. Disposizioni 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, comma 4, 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 DPCM 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'Agenzia per l'Italia Digitale (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)	Provvedimento generale prescrittivo in tema di biometrica – 12 novembre 2014	Provvedimento dell’Autorità Garante del 12 novembre 2014 pubblicato sulla Gazzetta Ufficiale n. 280 del 2 dicembre 2014 che riporta le informazioni e note prescrittive in tema di biometria.
(12)	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, di tipo grafometrico, 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 Clienti MyAzimut indicato sulla brochure informativa pubblicata sul sito internet di Azimut.

4.2 SOGGETTO CHE REALIZZA LA SOLUZIONE DI FIRMA GRAFOMETRICA

In aderenza a quanto espresso nell'Art, 55 comma 2 lettera b) del DCPM datato 22.2.2013, si segnala che la soluzione di Firma Grafometrica 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 SIGNificant. XYZMO Software GmbH opera da oltre 10 anni nei sistemi di acquisizione e trattamento dei dati calligrafici.

4.3 ALTRI 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 la soluzione di Firma Grafometrica SIGNificant di XYZMO e conserva presso il proprio Data Center i server XYZMO acquistati dalla **SGR** ma dei quali cura installazione, gestione e aggiornamento.

4.3.3 MAGNETIC MEDIA NETWORK SPA

Fornisce alla **SGR** le periferiche iPad indispensabili per l'erogazione del servizio, ne cura la sicurezza sia in fase di distribuzione sia da remoto durante l'utilizzazione stessa attraverso servizi di Mobile Device Management.

4.3.4 POSTEL SPA

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

4.3.5 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** al fine di gestire i servizi di Firma Elettronica Avanzata. Il documento recepisce quanto richiesto dalle Regole Tecniche del 22 febbraio 2013 e dal Provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014.

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, “**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 grafometria, 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 dematerializzare 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 PRIVACY

L'utilizzo di una soluzione di Firma Grafometrica, acquisendo dati biometrici benché solo comportamentali, ne implica il trattamento. Tali dati biometrici sono cifrati, come descritto nel paragrafo 12.6 del presente documento. Tali dati non sono utilizzabili né dal cliente utente, né dalla **SGR**.

La **SGR** è titolare del trattamento dei dati e provvederà, prima dell'avvio dell'operatività, a notificare il trattamento secondo le modalità previste dall'articolo 38 del Decreto Legislativo 196/2003 (“Codice Privacy”). Il Garante inserirà tale notifica nel registro dei trattamenti e, di conseguenza, tale notifica sarà accessibile utilizzando l'URL <http://www.garanteprivacy.it>. Le notizie accessibili consultando il registro

possono essere trattate per esclusiva finalità di applicazione della disciplina in materia di protezione dei dati personali.

La soluzione di FEA realizzata prevede l'utilizzo della Firma Grafometrica e, di conseguenza, la raccolta di dati biometrici. E' nostra opinione che l'utilizzo di questi dati sia solo funzionale alla firma e non se ne faccia un utilizzo eccessivo, in quanto questi dati non sono previsti in consultazione se non in caso di contenzioso sull'autenticità della firma apposta o su richiesta di forze dell'ordine o magistratura. Il processo realizzato prevede, infatti, la cifratura dei dati e le chiavi di decifratura sono mantenute da Aruba Spa in qualità di Certification Authority, con possibilità di richiesta solo a fronte di contenzioso o richiesta ufficiale dagli organi competenti per l'estrazione, da parte di un perito incaricato dalle parti, in luogo terzo e sicuro.

Considerando che la Firma Grafometrica raccoglie dati biometrici del sottoscrittore, nel contesto della garanzia della privacy, ci troviamo nell'applicazione dell'art 37, comma 1, lettera (a) del Codice Privacy; oltre a ciò il dato biometrico può essere visto come dato "quasi sensibile", pertanto, è opportuno tener conto anche dell'articolo 17. Ulteriore attenzione deve essere posta anche all'articolo 7 del Codice Privacy.

<p>Art. 37 – Notificazione del trattamento</p> <p>Comma 1) Il titolare notifica al Garante il trattamento di dati personali cui intende procedere, solo se il trattamento riguarda</p> <p>(a) Dati generici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica</p>	<p>La SGR provvede ad inserire la notifica a mezzo del portale del Garante nelle modalità standard, prima di iniziare l'operatività.</p>
<p>Art. 17 Trattamento che presenta rischi specifici</p> <ol style="list-style-type: none"> 1. Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità di trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti. 2. Le misure e gli accorgimenti di cui a comma 1 sono prescritti dal Garante in applicazione dei principi sanciti dal presente codice, nell'ambito di una verifica preliminare all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpellato del titolare 	<p>Il processo realizzato non prevede né permette la consultazione di dati biometrici acquisiti e, di conseguenza, non permette nessuna analisi di questi dati.</p>

<p>Art. 7 Diritto di accesso ai dati personali e altri diritti</p> <ol style="list-style-type: none"> 1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile 2. L'interessato ha diritto di ottenere l'indicazione: <ol style="list-style-type: none"> a) Dell'origine dei dati personali b) Delle finalità e modalità di trattamento 	<p>L'interessato sottoscrive una accettazione all'utilizzo della FEA e ha a disposizione una specifica informativa in modo da essere completamente informato sia del processo sia della raccolta dei dati. Potrà inoltre richiedere quanto sottoscritto come esplicitato nel paragrafo 10.5.</p>
--	--

9 FIRMA GRAFOMETRICA COME FIRMA ELETTRONICA AVANZATA

Per poter essere valida come FEA, la Firma Grafometrica 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, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima;
- 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 grafometrica adottata si configura come Firma Elettronica Avanzata

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

Identificazione del firmatario del documento	Il Consulente Finanziario segue la medesima operatività prevista per la stipula tramite documento cartaceo. In particolare identifica il firmatario a mezzo dei documenti di riconoscimento in corso di validità
Connessione univoca della firma con il firmatario	La firma grafometrica permette di acquisire la firma naturale del firmatario e dati vettoriali grafometrici che rendono univoca la firma e potrà essere analizzata con strumenti di verifica a disposizione del perito.
Controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima	La firma apposta unisce 3 strumenti che sono sotto il diretto controllo del firmatario (mano, tavoletta e dati biometrici). L'ambiente è in sicurezza e presidiato e ciò consente di effettuare senza dubbi le verifiche sull'apposizione dei dati biometrici apposti sul documento. In oltre 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 informata 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, in schermo dedicato, la visione completa del documento sottoposto a firma e può scorrelo 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 all'area riservata denominata MyAzimut.
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 dei 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
--	---

La soluzione adottata risponde positivamente a quanto richiesto, nel documento "Provvedimento generale prescrittivo in tema di biometria – 12 novembre 2014" in tema di sottoscrizione di documenti elettronici a mezzo di biometria.

PRESCRIZIONE
a) Il procedimento di firma è abilitato previa identificazione del firmatario.
b) Sono resi disponibili sistemi alternativi (cartacei o digitali) di sottoscrizione, che non comportino l'utilizzo di dati biometrici.
c) La cancellazione dei dati biometrici grezzi e dei campioni biometrici ha luogo immediatamente dopo il completamento della "procedura di sottoscrizione" e nessun dato biometrico persiste all'esterno del documento informatico sottoscritto.
d) I dati biometrici e grafometrici non sono conservati, neanche per periodi limitati, sui dispositivi hardware utilizzati per la raccolta, venendo memorizzati all'interno dei documenti informatici sottoscritti in forma cifrata tramite sistemi di crittografia a chiave pubblica.
e) La trasmissione dei dati biometrici tra sistemi hardware di acquisizione, postazioni informatiche e server avviene esclusivamente tramite canali di comunicazione resi sicuri con l'ausilio di tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita.
f) Sono adottate idonee misure e accorgimenti tecnici per contrastare i rischi di installazione di software e di modifica della configurazione delle postazioni informatiche e dei dispositivi, se non esplicitamente autorizzati.
g) I sistemi informatici sono protetti contro azioni di malware e sono, inoltre, adottati sistemi di firewall per la protezione perimetrale della rete e contro i tentativi di accesso abusivo ai dati.
h) Nel caso di utilizzo di sistemi di firma grafometrica nello scenario mobile o BYOD (Bring Your Own Device). Sono adottati idonei sistemi di gestione delle applicazioni o dei dispositivi mobili, con il ricorso a strumenti MDM (Mobile Device Management) o MAM (Mobile Application Management) o altri equivalenti al fine di isolare l'area di memoria dedicata all'applicazione biometrica, ridurre i rischi di installazione abusiva di software anche nella caso di modifica della configurazione dei dispositivi e contrastare l'azione di eventuali agenti malevoli (malware).
i) I sistemi di gestione impiegati nei trattamenti grafometrici adottano certificazioni digitali e policy di sicurezza che disciplinino, sulla base di criteri predeterminati, le condizioni di loro utilizzo sicuro (in particolare, rendendo disponibili funzionalità remote wiping applicabili nei casi di smarrimento o sottrazione dei dispositivi).

- | |
|---|
| j) L'accesso al modello grafometrico cifrato avviene esclusivamente tramite l'utilizzo della chiave privata detenuta dal soggetto terzo fiduciario, o da più soggetti, in caso di frazionamento della chiave stessa, e nei soli casi in cui si renda indispensabile per l'insorgenza di un contenzioso sull'autenticità della firma a seguito di richiesta dell'autorità giudiziaria. Le condizioni e le modalità di accesso alla firma grafometrica da parte del soggetto terzo di fiducia o da parte di tecnici qualificati sono dettagliate nell'informativa resa agli interessati e nella relazione tecnica successivamente citata. |
| k) È predisposta una relazione che descrive gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare, fornendo altresì la valutazione della necessità e della proporzionalità del trattamento del dato biometrico rispetto alle finalità. Tale relazione tecnica è conservata aggiornata, con verifica di controllo almeno annuale, per tutto il periodo di esercizio del sistema biometrico e mantenuta a disposizione del Garante |

La rispondenza a quanto richiesto è dettagliata in un'opportuna Relazione Tecnica" così come richiesto da punto k) paragrafo 4.4 del documento citato.

10 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.

10.1 IDENTIFICAZIONE DEL FIRMATARIO

L'identificazione del firmatario viene effettuata dagli operatori incaricati della **SGR** (Consulenti 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 dello 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.

10.2 INFORMARE L'UTENTE FIRMATARIO

I consulenti finanziari, in qualità di operatori della **SGR**, prima di procedere con la richiesta di accettazione dell'utilizzo del servizio FEA, procedono a informare il firmatario 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.

10.3 DICHIARAZIONE DI ACCETTAZIONE

I consulenti finanziari della **SGR** dopo aver adeguatamente informato il cliente firmatario, 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, modifiche di rapporto e consenso alla raccolta dei dati biometrici.

10.4 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.

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

Su richiesta del cliente effettuata mediante comunicazione scritta, la **SGR** si rende disponibile a fornire, senza oneri per il cliente, 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 senza la presenza dei dati biometrici al solo scopo di informazione.

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

10.6 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.

10.7 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.

10.8 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.

10.9 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.

11 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(cinquecentimila/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

12 LA SOLUZIONE AZIMUT

In tema di firma grafometrica, XYZMO ha prestato particolare attenzione alla sicurezza del dato biometrico acquisito. Infatti, mentre il firmatario esegue la firma, i dati biometrici che lo caratterizzano 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;
- Firmare con penna compatibile con schermi touch sul display del tablet nell'apposita area di firma;
- Confermare la firma apposta con la selezione **FATTO** dopo aver apposto la firma;
- Cancellare la firma apposta qualora non sia, a suo avviso, chiara utilizzando la selezione **RIPROVA** e poi ripetere la firma;
- Annullare l'operazione di firma qualora non sia più propenso a firmare il documento, con la selezione della funzione **CANCELLA**.

Con la conferma (funzione FATTO) 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 biometrici cifrati, la chiave ASE cifrata, il tratto grafico, il tipo di tablet utilizzato e l'impronta (HASH) del documento, sono inseriti nel documento PDF, alla fine del processo 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 biometrici 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.

Vengono utilizzati una serie di Application Server jboss che installati su server utilizzando Oracle Enterprise Linux e con l'ausilio di Database Oracle in RAC per la gestione delle applicazioni e le iterazioni con il SIGNificant Server.

12.1 IL SOFTWARE DI FIRMA

Per la realizzazione del servizio di Firma Elettronica Avanzata con Firma Grafometrica, **Azimut Capital Management SGR S.p.A.** ha utilizzato un software denominato SIGNificant di Xyzmo il cui client è installato sulla postazione mobile degli operatori della SGR (consulenti finanziari). La soluzione mobile è iPad.

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

12.2 IL SIGNIFICANT CLIENT

E' la componente inclusa nell' APP iOS installato sul dispositivo mobile del consulente ed ha il compito di ricevere e visualizzare i documenti da sottoporre all'utente firmatario, di acquisire i dati biometrici, di cifrarli insieme ad altre informazioni (chiave AES cifrata, tratto grafico e tipo di tablet) 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 biometrici dell'utente; 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.

12.3 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 biometrici li invia cifrati insieme ad altre informazioni al SIGNificant Server, il SIGNificant Server inserisce i dati biometrici cifrati, la chiave AES cifrata, il tratto grafico del firmatario ed il tipo di tablet 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.

12.4 MODALITÀ DI FIRMA

La soluzione adottata si basa sulla tecnologia Xyzmo e su una architettura che prevede l'installazione di una specifica APP su iPad rivolta ai consulenti finanziari del gruppo AZIMUT. Tale APP permette l'utilizzo della logica del SIGNificante Client di Xyzmo che comunica, solo in modalità On-Line e su canale sicuro HTTPS, con il SIGNificant Server di Xyzmo.

L'installazione della APP che incorpora il SIGNificante Client di Xyzmo viene consegnata da Obiectway a Magnetic Media Network e da loro installata mediante apposita procedura e utilizzando un sistema MDM (Mobile Device Management). La versione utilizzata di iOS è enterprise. Nello specifico, tale APP non è disponibile su Apple Store ma riservata solo alle persone autorizzate del gruppo Azimut.

La prima attività che viene richiesta al cliente, in modo che possa poi usufruire dei servizi di FEA in mobilità, è l'accettazione e sottoscrizione del consenso all'utilizzo della FEA e alla raccolta dei dati biometrici. Tale consenso viene raccolto dal Consulente dopo aver fatto leggere l'informativa al cliente.

Il secondo passo, propedeutico all'utilizzo del sistema in mobilità è il deposito, utilizzando il dispositivo mobile (tablet), degli specimen grafici di firma e dati biometrici per finalità di controllo in ipotesi di contenzioso. I dati, raccolti su apposito documento, saranno criptati con certificato asimmetrico, chiusi con certificato non qualificato e inviati in conservazione a norma. Tali documenti saranno utilizzabili, su richiesta degli organi giudiziari, solo in ipotesi di contenzioso dai periti grafometrici come documento di riferimento.

Per la sottoscrizione di documenti digitali da parte degli utenti, è necessario che il consulente, sempre presente alle sottoscrizioni, abbia inserito le proprie credenziali d'accesso sul dispositivo mobile, e deve essere stato riconosciuto dal sistema informativo della SGR.

All'utente firmatario sono sottoposti documenti digitali in formato PDF con uno o più campi firma; il campo firma viene presentato al sottoscrittore in modalità esplicita sul tablet e l'intero foglio del documento è disponibile e visualizzato sullo stesso.

L'utente firma grazie al cosiddetto "link effect" (il cui effetto grafico è quello di una classica firma sulla carta dove in realtà sono stati acquisiti i dati calligrafici biometrici), l'utente mantiene il controllo esclusivo dell'operazione di firma, premendo il tasto FATTO accetta l'invio dei dati biometrici crittografati che verranno poi inseriti sul documento opportunamente protetto.

I dati biometrici sono acquisiti dal SIGNificante 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.

12.5 LA SICUREZZA

In tema di firma grafometrica, XYZMO ha prestato particolare attenzione alla sicurezza del dato biometrico acquisito. Infatti, mentre il firmatario esegue la firma, i dati biometrici che lo caratterizzano 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;
- Firmare con penna compatibile con schermi touch sul display del tablet nell'apposita area di firma;
- Confermare la firma apposta con la selezione **FATTO** dopo aver apposto la firma;
- Cancellare la firma apposta qualora non sia, a suo avviso, chiara utilizzando la selezione **RIPROVA** e poi ripetere la firma;
- Annullare l'operazione di firma qualora non sia più propenso a firmare il documento, con la selezione della funzione **CANCELLA**.

Con la conferma (funzione FATTO) 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 biometrici cifrati, la chiave ASE cifrata, il tratto grafico, il tipo di tablet utilizzato e l'impronta (HASH) del documento, sono inseriti nel documento PDF, alla fine del processo 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 biometrici 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.

12.6 INTEGRITÀ DEL DOCUMENTO SOTTOSCRITTO

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

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

Il SIGNificant Server al termine dell'inserimento dei dati biometrici 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.

13 PROCESSO DI IDENTIFICAZIONE E FIRMA

Quando il consulente finanziario richiede al Cliente di apporre una o più firme autografe, 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 si potrà procedere all'apposizione della firma/e in forma grafometrica.

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 (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 deposita mediante il dispositivo mobile, in possesso del consulente finanziario (iPAD), lo specimen di firma al fine di consentire al perito grafometrico di avere un documento di riferimento in caso di contenziosi.

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).

13.1 DEPOSITO DELLE FIRME CONSULENTE

Per poter proporre documenti elettronici in modalità FEA, anche il consulente finanziario di Azimut deve accettare di procedere in tale senso. Se non accetta proseguirà a stipulare operazioni in formato cartaceo.

In prima istanza, il consulente che desidera aderire al servizio di FEA deve sottoscrivere la dichiarazione di accettazione delle condizioni di erogazione del servizio in cui viene riportato il processo di firma ai fini di recepire il consenso da parte del consulente. In particolare, il documento, deve segnalare che ci sarà una fase di deposito dello specimen di firma. Il consulente sarà quindi chiamato direttamente ad eseguire il deposito dello specimen di firma autocertificando che le firme inserite sono le sue.

Il processo di deposito dello specimen di firma è un processo preliminare che viene svolto direttamente dal consulente finanziario anche per quanto concerne la propria firma e prima di poter acquisire le firme del cliente.

In questa fase si provvede ad acquisire le 7 firme da riferire al consulente. Il consulente completa la procedura confermando l'operazione. Il documento così firmato potrà essere utilizzato dal perito grafometrico in caso di contenzioso.

In dettaglio, il consulente, tramite il dispositivo mobile (Tablet iPad), si identifica al sistema della SGR ed esegue l'accesso al sistema informativo aziendale con le proprie credenziali.

Seleziona la funzione di raccolta dello specimen di firma e inizia le operazioni.

Dopo avere verificato che i suoi dati sono corretti in anagrafica procede con la firma del documento di deposito dello specimen di firma e conferma le firme apposte con il tasto "Fatto". Il processo eseguito è il seguente ovvero Il SIGNificant Client propone un'immagine ottimizzata del pdf ricevuto dall'applicazione (pdf su cui il SIGNificant Server ha calcolato l'impronta "hash" del documento) e presenta il campo di firma, raccoglie i tratti grafici e biometrici del firmatario, mentre viene eseguita la firma, i dati raccolti sono cifrati nella memoria del dispositivo mobile con chiave simmetrica AES. Tale chiave è generata in modo casuale dal SIGNificant Client. Tal chiave viene a sua volta cifrata con chiave pubblica RSA:

Durante questa operazione il firmatario ha il completo ed esclusivo controllo del processo di firma attraverso le seguenti funzioni:

- Controllo della firma che appone direttamente su tablet con penna compatibile con schermi touch nell'apposito campo firma del documento di deposito dello specimen di firma;
- Conferma della firma apposta mediante la selezione del campo **FATTO**;
- Cancellazione del tratto grafico per la ripetizione della firma con la selezione del campo **RIPROVA**;
- Annullare l'operazione della firma selezionando il campo **CANCELLA**.

Con la selezione del campo FATTO il firmatario conferma la firma apposta, Il SIGNificant Client invia i dati al SIGNificant Server.

Le firme sono raccolte in un documento che viene chiuso con un certificato a nome della società e inviato in archiviazione a norma e inviata immagine, via e-mail al consulente finanziario. In caso di errore tutti i dati sono cancellati e si segnala di ripetere tutta la procedura dall'inizio.

13.2 DEPOSITO DELLE FIRME CLIENTE

Il processo di deposito dello specimen di firma è un processo preliminare che viene svolto dal consulente e dal cliente.

In questa fase, il consulente, provvede ad informare, dando piena disponibilità della documentazione prodotta dal gruppo Azimut, al processo di sottoscrizione con FEA. 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. Completata

questa fase si può procedere a depositare lo specimen di firma del cliente. Il consulente completa la procedura applicando la sua firma (in modalità Firma Grafometrica) al fine di garantire che l'operazione sia stata eseguita in sua presenza.

In dettaglio, il consulente, tramite il dispositivo mobile (Tablet iPad), si identifica al sistema della SGR ed esegue l'accesso al sistema informativo aziendale con le proprie credenziali.

Seleziona la funzione di deposito dello specimen di firma e inizia le operazioni.

Dopo avere verificato tutte le informazioni relative al cliente si procede con la raccolta delle firme. Il processo eseguito è il seguente:

Il SIGNificant Client propone un'immagine ottimizzata del pdf ricevuto dall'applicazione (pdf su cui il SIGNificant Server ha calcolato l'impronta "hash" del documento) e propone il campo di firma e raccoglie i tratti grafici e biometrici del firmatario, mentre viene eseguita la firma, i dati raccolti sono cifrati nella memoria del dispositivo mobile con chiave simmetrica AES. Tale chiave è generata in modo casuale dal SIGNificant Client. Tal chiave viene a sua volta cifrata con chiave pubblica RSA:

Durante questa operazione il firmatario ha il completo ed esclusivo controllo del processo di firma attraverso le seguenti funzioni:

- Controllo della firma che appone direttamente su tablet con penna compatibile con schermi touch nell'apposito campo firma del documento di deposito dello specimen di firma;
- Conferma della firma apposta mediante la selezione del campo **FATTO**;
- Cancellazione del tratto grafico per la ripetizione della firma con la selezione del campo **RIPROVA**;
- Annullare l'operazione della firma selezionando il campo **CANCELLA**.

Con la selezione del campo FATTO il firmatario conferma la firma apposta, Il SIGNificant Client invia i dati al SIGNificant Server e riprende a chiedere l'ulteriore firma.

Le firme sono raccolte nel documento di specimen di firma che viene chiuso con un certificato a nome della società e copia del suddetto documento viene inviata al cliente utilizzando l'indirizzo di mail comunicato dal cliente. In caso di errore o annullamento tutti i dati sono cancellati e si segnala di ripetere tutta la procedura dall'inizio.

Si evidenzia che la firma del consulente finanziario a conclusione della fase di firma serve ad attestare che ha riconosciuto il cliente ed seguito direttamente il processo.

13.3 IL PROCESSO DI FIRMA

I SIGNificant Client e SIGNificant Server sono in grado di firmare documenti in formato PDF con firma autografa, 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 il dispositivo mobile, si identifica al sistema della SGR ed esegue l'accesso al sistema informativo del Gruppo Azimut con le proprie credenziali;
- Il consulente compila, richiede o seleziona il documento che desidera far sottoscrivere al cliente;
- Viene quindi inviato al dispositivo mobile il documento PDF compilato da far sottoscrivere al cliente;
- Il SIGNificant Client inoltra il documento PDF 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 dispositivo mobile del consulente che attiva il processo di firma per il firmatario.

Il firmatario 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;
- Firma con la penna compatibile con schermi touch sul display del tablet nell'apposita area di firma;
- (**FATTO**) confermare la firma apposta;
- (**RIPROVA**) cancellare il tratto grafico della firma per riscriverla;
- (**CANCELLA**) annullare l'inserimento della firma.

Mentre il sottoscrittore esegue la firma, i dati biometrici che lo caratterizzano 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 RSA (a chiavi asimmetriche).

Con la conferma (**FATTO**) da parte del firmatario il SIGNificant Client invia al SIGNificant Server, i dati biometrici cifrati, la chiave AES cifrata, il tratto grafico ed il tipo di tablet utilizzato. Il SIGNificant Server:

- Inserisce i dati ricevuti dal SIGNificant Client nel documento PDF originale residente sul server;

- Invia al SIGNificant Client l'immagine PDF ottimizzata del documento, con il tratto grafico 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 consulente finanziario appone la propria sottoscrizione mediante firma grafometrica in conclusione delle operazioni di acquisizione delle firme del cliente. Tale firma viene gestita con la medesima operatività illustrata per la firma del cliente. Dopo che tutte le firme sono state apposte l'utente conferma la conclusione della sottoscrizione del documento.

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 e-mail o nell'area riservata MyAzimut).

13.4 LE COMUNICAZIONI CIFRATE

La comunicazione ed il trasferimento dei dati biometrici 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 biometrici tra il Client ed il Server sono su un canale HTTPS (criptato) con algoritmo asimmetrico.

14 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.

14.1 CHIAVE PUBBLICA DI CIFRATURA

I dati biometrici 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.

14.2 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.

14.3 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.

14.4 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.

15 COMPONENTI DI SICUREZZA

15.1 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.

15.2 DEVICE

Nell'ambito del progetto Azimut ha deciso di adottare la soluzione AirWatch acquisendo il servizio da Magnetic Media Network.

MMN offre un servizio di Mobile Device Management tramite la piattaforma AirWatch, tramite la quale è possibile effettuare il controllo e la configurazione degli apparati ad uso della rete, la distribuzione di applicazioni e contenuti in modo sicuro ed efficiente.

- Il sistema è in grado di controllare apparati diversi in termini di sistemi operativi, in questo caso si prevede utilizzo solo di apparati iOS.
- Il servizio minimo comprende l'attivazione degli apparati e la configurazione di base degli stessi.
- Sono disponibili diverse interfacce di accesso al sistema che può essere utilizzato anche "as-a-service" da parte del personale della **SGR** o di **ObjectWay**.

In fase di rilascio degli apparati, viene effettuata la configurazione tramite un "profilo base" che prevede i seguenti parametri:

- Obbligo dell'uso di un PIN per lo sblocco dell'apparato.
- Blocco del backup e del trasferimento di dati "aziendali".

In particolare, per i device iOS i dispositivi saranno affidati, attraverso relativa procedura di iscrizione, al sistema *AirWatch* il quale si occuperà della loro gestione e controllo. Il sistema *AirWatch* effettua una verifica costante dei dispositivi per accertarne la conformità. Tale conformità prevede che lo stesso soddisfi determinate caratteristiche tra le quali:

- Codice di blocco presente.
- Memoria criptata.

La verifica di questi requisiti garantisce che il dispositivo, il sistema operativo e tutte le applicazioni in esso contenute siano originali e certificate. Garantisce che il dispositivo non sia utilizzabile se non attraverso il possesso del codice di sblocco.

E' altresì garantito che le applicazioni pubbliche (gratuite o a pagamento) possono essere installate esclusivamente dallo store di Apple. Mentre per quanto riguarda le applicazioni aziendali, non veicolate dallo store di Apple, garantisce che siano state firmate con un certificato enterprise valido prima di essere distribuite e installate.

In caso di furto, previa richiesta o accordo con **Azimut Capital Management SGR S.p.A.**, la soluzione di MDM potrà effettuare la cancellazione remota parziale (solo dati aziendali) o totale (dati aziendali e personali).

I dati su dispositivi iOS (iPAD , iPhone) sono conservati all'interno del dispositivo in forma criptata, accessibile solo a fronte di sblocco tramite codice.

Il dispositivo è gestito attraverso AirWatch, grazie al quale è possibile, in caso di furto o smarrimento e a fronte di specifica richiesta o accordo, effettuare il Remote-Enterprise-WIPE ossia la cancellazione dei dati aziendali (configurazioni e applicazioni) dal dispositivo. Questa operazione è veicolata attraverso la connessione internet ed ha effetto immediato

L'utente ha sempre la facoltà di scollegare il dispositivo dal sistema MDM, attraverso la semplice rimozione di un profilo di configurazione. Tale pratica tuttavia rimuove tutte le configurazioni, le applicazioni aziendali e i dati rilasciati dall'azienda, rendendo di fatto il dispositivo inutilizzabile ai fini lavorativi.

16 ARCHIVIAZIONE E CONSERVAZIONE A NORMA DEI DOCUMENTI

Il processo di archiviazione, datacertazione 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:

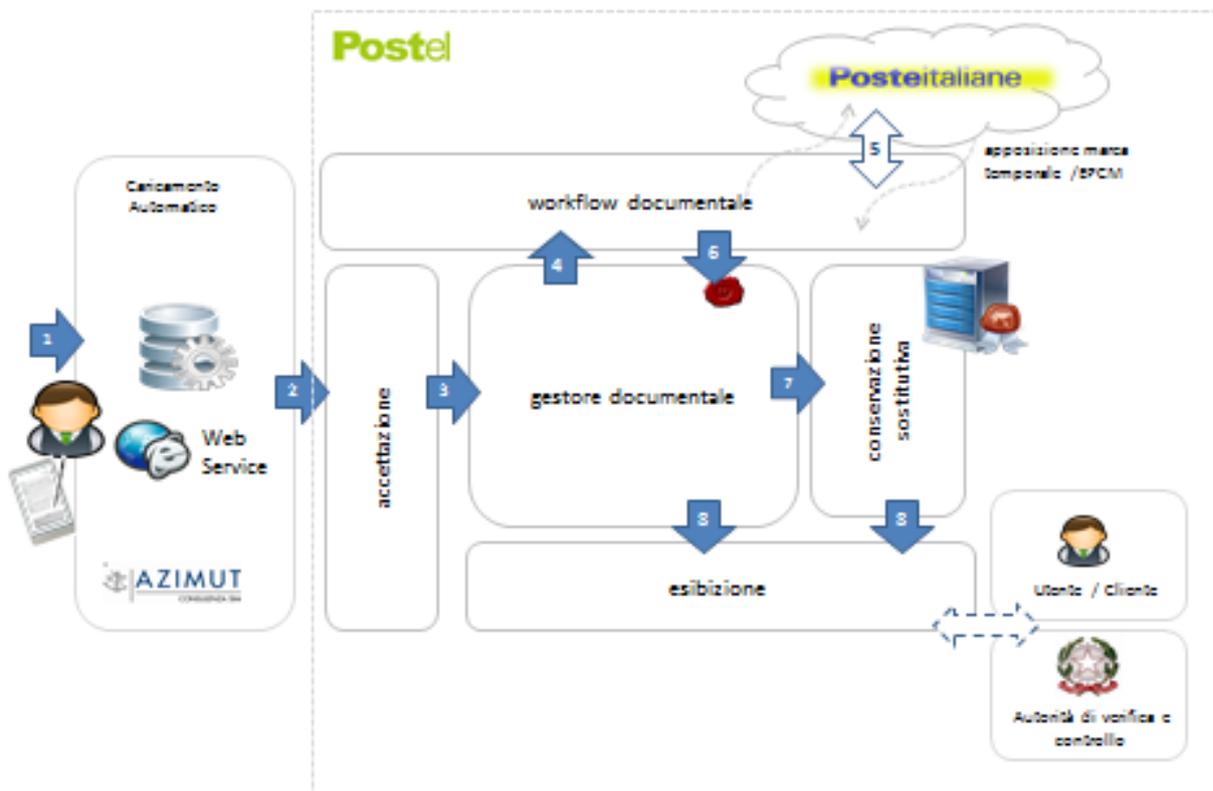
- Reverse Proxy IBM http Server 6.1, Apache web server (RP1),
- Data Server Oracle 10G in alta affidabilità (PB1, PB2),
- Content Serve con SO Red Hat Enterprise Linux 5.0 (CS1,CS2),
- Application Server con SO Red Hat Enterprise Linux 5.0 e Web Server IBM WS 6 (WS1, Ws2),
- Storage dati di tipo SAN (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 biometrici, 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 Status OK)
ErrorMessage	String	Messaggio di errore ritornato da web service (valorizzato solo se Status OK)

17 LA GESTIONE DEL CONTENZIOSO

Il processo di gestione di un contenzioso, inizialmente segue le classiche politiche di gestione previste dall'istituto ma, in ipotesi che il contenzioso veda l'intervento di giudici per risolverlo, si deve obbligatoriamente prevedere un diverso approccio di perizia.

In particolare è necessario procedere ad una perizia dei dati informatici e biometrici delle firme in contenzioso.

Per questo motivo Xyzmo mette a disposizione un software che permette il confronto dei dati biometrici e informatici della firma nonché la visione 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 contestato e del documento di deposito degli specimen di firma;
- 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 fa apporre una nuova firma al cliente e la analizza confrontando i dati sia con il documento contestato sia con gli specimen di firma ed eventualmente con altri documenti firmati entro un periodo di un anno.

Manuale Operativo

Manuale Operativo
Firma Elettronica Avanzata FEA
Firma Grafometrica
Azimut Financial Insurance S.p.A.

Data	1 Ottobre 2016
Versione	1.3
Stato	Definitivo

1 SOMMARIO

1	Sommario	2
2	Premessa	5
3	Definizioni.....	6
3.1	Definizioni riguardanti i soggetti	6
3.2	Acronimi, definizioni e termini utilizzati.....	7
3.3	Riferimenti Normativi.....	10
4	Gli attori.....	12
4.1	Soggetto che eroga la soluzione.....	12
4.1.1	Dati Identificativi.....	12
4.1.2	Assistenza Cliente	12
4.2	Soggetto che realizza la soluzione di Firma Grafometrica.....	13
4.3	Altri soggetti coinvolti.....	13
4.3.1	Studio Legale Zitiello e Associati.....	13
4.3.2	Objectway Financial Software SPA	13
4.3.3	Magnetic Media Network SPA.....	13
4.3.4	Postel SPA	13
4.3.5	Actalis SPA.....	13
5	Scopo del Documento	14
6	Finalità.....	15
7	Quadro Normativo	15
8	Privacy	15
9	Firma grafometrica come firma elettronica avanzata	17
10	Obblighi	20
10.1	Identificazione del firmatario.....	21
10.2	Informare l'utente firmatario.....	21
10.3	Dichiarazione di accettazione	22

10.4	Conservazione documenti richiesti	22
10.5	Garanzia di disponibilità, integrità e leggibilità del documento di accettazione del servizio e messa a disposizione gratuita del documento di accettazione.....	22
10.6	Caratteristiche del sistema di firma	22
10.7	La tecnologia utilizzata	22
10.8	Pubblicazione sul sito	23
10.9	Servizio di revoca	23
11	Tutela assicurativa.....	23
12	La soluzione Azimut.....	24
12.1	Il Software di Firma	25
12.2	Il SIGNificant Client.....	25
12.3	Il SIGNificant Server.....	25
12.4	Modalità di firma.....	26
12.5	La sicurezza	27
12.6	Integrità del documento sottoscritto.....	28
13	Processo di Identificazione e firma	29
13.1	Deposito delle Firme Addetto all'attività di intermediazione.....	29
13.2	Deposito delle Firme Cliente	30
13.3	Il processo di firma	32
13.4	Le comunicazioni cifrate.....	34
14	Altri componenti	35
14.1	Chiave Pubblica di Cifratura	35
14.2	Chiave Privata di Cifratura.....	35
14.3	Certificato di firma	35
14.4	Marca Temporale	35
15	Componenti di sicurezza	36
15.1	Server	36
15.2	Device.....	36

16	Archiviazione e conservazione a norma dei documenti	38
17	La gestione del contenzioso	42

2 PREMESSA

Il presente documento riporta le informazioni relative al progetto di Firma Elettronica Avanzata con Firma Grafometrica 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 acquisizione 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 della 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	È 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. È 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 della 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.
Signature Tablet	Dispositivo elettronico che si connette ad un computer ed è in grado di acquisire dati biometrici comportamentali e grafici di una firma autografa. I valori acquisiti sono coordinate x-y; tempo; eventuale pressione.
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 DL 235/2010
Tablet	Dispositivo mobile (es. iPad) in grado di acquisire i dati biometrici di una firma autografa per mezzo di specifiche penne elettroniche.

3.3 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, comma 4, 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 DPCM 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'Agenzia per l'Italia Digitale (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)	Provvedimento generale prescrittivo in tema di biometrica – 12 novembre 2014	Provvedimento dell’Autorità Garante del 12 novembre 2014 pubblicato sulla Gazzetta Ufficiale n. 280 del 2 dicembre 2014 che riporta le informazioni e note prescrittive in tema di biometria.
(12)	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, di tipo grafometrico, 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 l'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 GRAFOMETRICA

In aderenza a quanto espresso nell'Art. 55 comma 2 lettera b) del DCPM datato 22.2.2013, si segnala che la soluzione di Firma Grafometrica 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 SIGNificant. XYZMO Software GmbH opera da oltre 10 anni nei sistemi di acquisizione e trattamento dei dati calligrafici.

4.3 ALTRI 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 e di distribuzione di prodotti e servizi bancari integrando la soluzione di Firma Grafometrica SIGNificant di XYZMO e conserva presso il proprio Data Center i server XYZMO acquistati dalla **AFI** ma dei quali cura installazione, gestione e aggiornamento.

4.3.3 MAGNETIC MEDIA NETWORK SPA

Fornisce alla **AFI** le periferiche iPad indispensabili per l'erogazione del servizio, ne cura la sicurezza sia in fase di distribuzione sia da remoto durante l'utilizzazione stessa attraverso servizi di Mobile Device Management.

4.3.4 POSTEL SPA

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

4.3.5 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** al fine di gestire i servizi di Firma Elettronica Avanzata. Il documento recepisce quanto richiesto dalle Regole Tecniche del 22 febbraio 2013 e dal Provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014.

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, “**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 grafometria, 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 dematerializzare 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 PRIVACY

L'utilizzo di una soluzione di Firma Grafometrica, acquisendo dati biometrici benché solo comportamentali, ne implica il trattamento. Tali dati biometrici sono cifrati, come descritto nel paragrafo 12.6 del presente documento. Tali dati non sono utilizzabili né dal cliente utente, né dalla **AFI**.

La **AFI** è titolare del trattamento dei dati e provvederà, prima dell'avvio dell'operatività, a notificare il trattamento secondo le modalità previste dall'articolo 38 del Decreto Legislativo 196/2003 (**“Codice Privacy”**). Il Garante inserirà tale notifica nel registro dei trattamenti e, di conseguenza, tale notifica sarà accessibile utilizzando l'URL <http://www.garanteprivacy.it>. Le notizie accessibili consultando il registro

possono essere trattate per esclusiva finalità di applicazione della disciplina in materia di protezione dei dati personali.

La soluzione di FEA realizzata prevede l'utilizzo della Firma Grafometrica e, di conseguenza, la raccolta di dati biometrici. E' nostra opinione che l'utilizzo di questi dati sia solo funzionale alla firma e non se ne faccia un utilizzo eccessivo, in quanto questi dati non sono previsti in consultazione se non in caso di contenzioso sull'autenticità della firma apposta o su richiesta di forze dell'ordine o magistratura. Il processo realizzato prevede, infatti, la cifratura dei dati e le chiavi di decifratura sono mantenute da Aruba Spa in qualità di Certification Authority, con possibilità di richiesta solo a fronte di contenzioso o richiesta ufficiale, dagli organi competenti per l'estrazione, da parte di un perito incaricato dalle parti, in luogo terzo e sicuro.

Considerando che la Firma Grafometrica raccoglie dati biometrici del sottoscrittore, nel contesto della garanzia della privacy, ci troviamo nell'applicazione dell'art 37, comma 1, lettera (a) del Codice Privacy; oltre a ciò il dato biometrico può essere visto come dato "quasi sensibile", pertanto, è opportuno tener conto anche dell'articolo 17. Ulteriore attenzione deve essere posta anche all'articolo 7 del Codice Privacy.

<p>Art. 37 – Notificazione del trattamento</p> <p>Comma 1) Il titolare notifica al Garante il trattamento di dati personali cui intende procedere, solo se il trattamento riguarda</p> <p>(a) Dati generici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica</p>	<p>La AFI provvede ad inserire la notifica a mezzo del portale del Garante nelle modalità standard, prima di iniziare l'operatività.</p>
<p>Art. 17 Trattamento che presenta rischi specifici</p> <ol style="list-style-type: none"> 1. Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità di trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti. 2. Le misure e gli accorgimenti di cui a comma 1 sono prescritti dal Garante in applicazione dei principi sanciti dal presente codice, nell'ambito di una verifica preliminare all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare 	<p>Il processo realizzato non prevede né permette la consultazione di dati biometrici acquisiti e, di conseguenza, non permette nessuna analisi di questi dati.</p>

<p>Art. 7 Diritto di accesso ai dati personali e altri diritti</p> <ol style="list-style-type: none"> 1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile 2. L'interessato ha diritto di ottenere l'indicazione: <ol style="list-style-type: none"> a) Dell'origine dei dati personali b) Delle finalità e modalità di trattamento 	<p>L'interessato sottoscrive una accettazione all'utilizzo della FEA e ha a disposizione una specifica informativa in modo da essere completamente informato sia del processo sia della raccolta dei dati. Potrà inoltre richiedere quanto sottoscritto come esplicitato nel paragrafo 10.5.</p>
--	--

9 FIRMA GRAFOMETRICA COME FIRMA ELETTRONICA AVANZATA

Per poter essere valida come FEA, la Firma Grafometrica 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, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima;
- 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 grafometrica adottata si configura come Firma Elettronica Avanzata

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

Identificazione del firmatario del documento	L'Addetto all'attività di intermediazione segue la medesima operatività prevista per la stipula tramite documento cartaceo. In particolare identifica il firmatario a mezzo dei documenti di riconoscimento in corso di validità
Connessione univoca della firma con il firmatario	La firma grafometrica permette di acquisire la firma naturale del firmatario e dati vettoriali grafometrici che rendono univoca la firma e potrà essere analizzata con strumenti di verifica a disposizione del perito.
Controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima	La firma apposta unisce 3 strumenti che sono sotto il diretto controllo del firmatario (mano, tavoletta e dati biometrici). L'ambiente è in sicurezza e presidiato e ciò consente di effettuare senza dubbi le verifiche sull'apposizione dei dati biometrici apposti sul documento. In oltre 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 informata 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, in schermo dedicato, 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 all'area riservata denominata MyAzimut.
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 dei 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
--	---

La soluzione adottata risponde positivamente a quanto richiesto, nel documento "Provvedimento generale prescrittivo in tema di biometria – 12 novembre 2014" in tema di sottoscrizione di documenti elettronici a mezzo di biometria.

PRESCRIZIONE	
a)	Il procedimento di firma è abilitato previa identificazione del firmatario.
b)	Sono resi disponibili sistemi alternativi (cartacei o digitali) di sottoscrizione, che non comportino l'utilizzo di dati biometrici.
c)	La cancellazione dei dati biometrici grezzi e dei campioni biometrici ha luogo immediatamente dopo il completamento della "procedura di sottoscrizione" e nessun dato biometrico persiste all'esterno del documento informatico sottoscritto.
d)	I dati biometrici e grafometrici non sono conservati, neanche per periodi limitati, sui dispositivi hardware utilizzati per la raccolta, venendo memorizzati all'interno dei documenti informatici sottoscritti in forma cifrata tramite sistemi di crittografia a chiave pubblica.
e)	La trasmissione dei dati biometrici tra sistemi hardware di acquisizione, postazioni informatiche e server avviene esclusivamente tramite canali di comunicazione resi sicuri con l'ausilio di tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita.
f)	Sono adottate idonee misure e accorgimenti tecnici per contrastare i rischi di installazione di software e di modifica della configurazione delle postazioni informatiche e dei dispositivi, se non esplicitamente autorizzati.
g)	I sistemi informatici sono protetti contro azioni di malware e sono, inoltre, adottati sistemi di firewall per la protezione perimetrale della rete e contro i tentativi di accesso abusivo ai dati.
h)	Nel caso di utilizzo di sistemi di firma grafometrica nello scenario mobile o BYOD (Bring Your Own Device). Sono adottati idonei sistemi di gestione delle applicazioni o dei dispositivi mobili, con il ricorso a strumenti MDM (Mobile Device Management) o MAM (Mobile Application Management) o altri equivalenti al fine di isolare l'area di memoria dedicata all'applicazione biometrica, ridurre i rischi di installazione abusiva di software anche nella caso di modifica della configurazione dei dispositivi e contrastare l'azione di eventuali agenti malevoli (malware).
i)	I sistemi di gestione impiegati nei trattamenti grafometrici adottano certificazioni digitali e policy di sicurezza che disciplinino, sulla base di criteri predeterminati, le condizioni di loro utilizzo sicuro (in particolare, rendendo disponibili funzionalità remote wiping applicabili nei casi di smarrimento o sottrazione dei dispositivi).

- | |
|---|
| j) L'accesso al modello grafometrico cifrato avviene esclusivamente tramite l'utilizzo della chiave privata detenuta dal soggetto terzo fiduciario, o da più soggetti, in caso di frazionamento della chiave stessa, e nei soli casi in cui si renda indispensabile per l'insorgenza di un contenzioso sull'autenticità della firma a seguito di richiesta dell'autorità giudiziaria. Le condizioni e le modalità di accesso alla firma grafometrica da parte del soggetto terzo di fiducia o da parte di tecnici qualificati sono dettagliate nell'informativa resa agli interessati e nella relazione tecnica successivamente citata. |
| k) È predisposta una relazione che descrive gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare, fornendo altresì la valutazione della necessità e della proporzionalità del trattamento del dato biometrico rispetto alle finalità. Tale relazione tecnica è conservata aggiornata, con verifica di controllo almeno annuale, per tutto il periodo di esercizio del sistema biometrico e mantenuta a disposizione del Garante |

La rispondenza a quanto richiesto è dettagliata in un'opportuna Relazione Tecnica" così come richiesto da punto k) paragrafo 4.4 del documento citato.

10 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.

10.1 IDENTIFICAZIONE DEL FIRMATARIO

L'identificazione del firmatario 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 dello 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.

10.2 INFORMARE L'UTENTE FIRMATARIO

Gli Addetti all'attività di intermediazione, in qualità di operatori della **AFI**, prima di procedere con la richiesta di accettazione dell'utilizzo del servizio FEA, procedono a informare il firmatario 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.

10.3 DICHIARAZIONE DI ACCETTAZIONE

Gli Addetti all'attività di intermediazione della **AFI** dopo aver adeguatamente informato il cliente firmatario, 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, modifiche di rapporto e consenso alla raccolta dei dati biometrici.

10.4 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.

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

Su richiesta del cliente effettuata mediante comunicazione scritta, la **AFI** si rende disponibile a fornire, senza oneri per il cliente, 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 senza la presenza dei dati biometrici 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.

10.6 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.

10.7 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.

10.8 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.

10.9 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 Addetto all'attività di intermediazione di riferimento o direttamente la **AFI** per ricevere assistenza per attivare le richiesta di Revoca.

11 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(cinquecentimila/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

12 LA SOLUZIONE AZIMUT

In tema di firma grafometrica, XYZMO ha prestato particolare attenzione alla sicurezza del dato biometrico acquisito. Infatti, mentre il firmatario esegue la firma, i dati biometrici che lo caratterizzano 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;
- Firmare con penna compatibile con schermi touch sul display del tablet nell'apposita area di firma;
- Confermare la firma apposta con la selezione **FATTO** dopo aver apposto la firma;
- Cancellare la firma apposta qualora non sia, a suo avviso, chiara utilizzando la selezione **RIPROVA** e poi ripetere la firma;
- Annullare l'operazione di firma qualora non sia più propenso a firmare il documento, con la selezione della funzione **CANCELLA**.

Con la conferma (funzione FATTO) 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 biometrici cifrati, la chiave ASE cifrata, il tratto grafico, il tipo di tablet utilizzato e l'impronta (HASH) del documento, sono inseriti nel documento PDF, alla fine del processo 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 biometrici 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.

Vengono utilizzati una serie di Application Server jboss che installati su server utilizzando Oracle Enterprise Linux e con l'ausilio di Database Oracle in RAC per la gestione delle applicazioni e le iterazioni con il SIGNificant Server.

12.1 IL SOFTWARE DI FIRMA

Per la realizzazione del servizio di Firma Elettronica Avanzata con Firma Grafometrica, **Azimut Financial Insurance S.p.A.** ha utilizzato un software denominato SIGNificant di Xyzmo il cui client è installato sulla postazione mobile degli operatori della AFI (Addetti all'attività di intermediazione). La soluzione mobile è iPad.

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

12.2 IL SIGNIFICANT CLIENT

E' la componente inclusa nell' APP iOS installato sul dispositivo mobile dell' Addetto all'attività di intermediazione ed ha il compito di ricevere e visualizzare i documenti da sottoporre all'utente firmatario, di acquisire i dati biometrici, di cifrarli insieme ad altre informazioni (chiave AES cifrata, tratto grafico e tipo di tablet) 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 biometrici dell'utente; 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.

12.3 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 biometrici li invia cifrati insieme ad altre informazioni al SIGNificant Server, il SIGNificant Server inserisce i dati biometrici cifrati, la chiave AES cifrata, il tratto grafico del firmatario ed il tipo di tablet 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.

12.4 MODALITÀ DI FIRMA

La soluzione adottata si basa sulla tecnologia Xyzmo e su una architettura che prevede l'installazione di una specifica APP su iPad rivolta agli Addetti all'attività di intermediazione del gruppo AZIMUT. Tale APP permette l'utilizzo della logica del SIGNificante Client di Xyzmo che comunica, solo in modalità On-Line e su canale sicuro HTTPS, con il SIGNificant Server di Xyzmo.

L'installazione della APP che incorpora il SIGNificant Client di Xyzmo viene consegnata da Obiectway a Magnetic Media Network e da loro installata mediante apposita procedura e utilizzando un sistema MDM (Mobile Device Management). La versione utilizzata di iOS è enterprise. Nello specifico, tale APP non è disponibile su Apple Store ma riservata solo alle persone autorizzate del gruppo Azimut.

La prima attività che viene richiesta al cliente, in modo che possa poi usufruire dei servizi di FEA in mobilità, è l'accettazione e sottoscrizione del consenso all'utilizzo della FEA e alla raccolta dei dati biometrici. Tale consenso viene raccolto dall' Addetto all'attività di intermediazione dopo aver fatto leggere l'informativa al cliente.

Il secondo passo, propedeutico all'utilizzo del sistema in mobilità è il deposito, utilizzando il dispositivo mobile (tablet), degli specimen grafici di firma e dati biometrici per finalità di controllo in ipotesi di contenzioso. I dati, raccolti su apposito documento, saranno criptati con certificato asimmetrico, chiusi con certificato non qualificato e inviati in conservazione a norma. Tali documenti saranno utilizzabili, su richiesta degli organi giudiziari, solo in ipotesi di contenzioso dai periti grafometrici come documento di riferimento.

Per la sottoscrizione di documenti digitali da parte degli utenti, è necessario che l'Addetto all'attività di intermediazione, sempre presente alle sottoscrizioni, abbia inserito le proprie credenziali d'accesso sul dispositivo mobile, e deve essere stato riconosciuto dal sistema informativo della AFI.

All'utente firmatario sono sottoposti documenti digitali in formato PDF con uno o più campi firma; il campo firma viene presentato al sottoscrittore in modalità esplicita sul tablet e l'intero foglio del documento è disponibile e visualizzato sullo stesso.

L'utente firma grazie al cosiddetto "link effect" (il cui effetto grafico è quello di una classica firma sulla carta dove in realtà sono stati acquisiti i dati calligrafici biometrici), l'utente mantiene il controllo esclusivo dell'operazione di firma, premendo il tasto FATTO accetta l'invio dei dati biometrici crittografati che verranno poi inseriti sul documento opportunamente protetto.

I dati biometrici 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.

12.5 LA SICUREZZA

In tema di firma grafometrica, XYZMO ha prestato particolare attenzione alla sicurezza del dato biometrico acquisito. Infatti, mentre il firmatario esegue la firma, i dati biometrici che lo caratterizzano 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;
- Firmare con penna compatibile con schermi touch sul display del tablet nell'apposita area di firma;
- Confermare la firma apposta con la selezione **FATTO** dopo aver apposto la firma;
- Cancellare la firma apposta qualora non sia, a suo avviso, chiara utilizzando la selezione **RIPROVA** e poi ripetere la firma;
- Annullare l'operazione di firma qualora non sia più propenso a firmare il documento, con la selezione della funzione **CANCELLA**.

Con la conferma (funzione FATTO) 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 biometrici cifrati, la chiave ASE cifrata, il tratto grafico, il tipo di tablet utilizzato e l'impronta (HASH) del documento, sono inseriti nel documento PDF, alla fine del processo 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 biometrici 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.

12.6 INTEGRITÀ DEL DOCUMENTO SOTTOSCRITTO

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

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

Il SIGNificant Server al termine dell'inserimento dei dati biometrici 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.

13 PROCESSO DI IDENTIFICAZIONE E FIRMA

Quando l'Addetto all'attività di intermediazione richiede al Cliente di apporre una o più firme autografe, 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 si potrà procedere all'apposizione della firma/e in forma grafometrica.

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, 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 (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 deposita mediante il dispositivo mobile, in possesso dell' Addetto all'attività di intermediazione (iPAD), lo specimen di firma al fine di consentire al perito grafometrico di avere un documento di riferimento in caso di contenziosi.

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).

13.1 DEPOSITO DELLE FIRME ADDETTO ALL'ATTIVITÀ DI INTERMEDIAZIONE

Per poter proporre documenti elettronici in modalità FEA, anche l'Addetto all'attività di intermediazione di AFI deve accettare di procedere in tale senso. Se non accetta proseguirà a stipulare operazioni in formato cartaceo.

In prima istanza, l'Addetto all'attività di intermediazione che desidera aderire al servizio di FEA deve sottoscrivere la dichiarazione di accettazione delle condizioni di erogazione del servizio in cui viene riportato il processo di firma ai fini di recepire il consenso da parte dell'Addetto all'attività di intermediazione. In particolare, il documento, deve segnalare che ci sarà una fase di deposito dello specimen di firma. L'Addetto all'attività di intermediazione sarà quindi chiamato direttamente ad eseguire il deposito dello specimen di firma autocertificando che le firme inserite sono le sue.

Il processo di deposito dello specimen di firma è un processo preliminare che viene svolto direttamente dall'Addetto all'attività di intermediazione anche per quanto concerne la propria firma e prima di poter acquisire le firme del cliente.

In questa fase si provvede ad acquisire le 7 firme da riferire all' Addetto all'attività di intermediazione. L'Addetto completa la procedura confermando l'operazione. Il documento così firmato potrà essere utilizzato dal perito grafometrico in caso di contenzioso.

In dettaglio, l'Addetto all'attività di intermediazione, tramite il dispositivo mobile (Tablet iPad), si identifica al sistema della AFI ed esegue l'accesso al sistema informativo aziendale con le proprie credenziali.

Seleziona la funzione di raccolta dello specimen di firma e inizia le operazioni.

Dopo avere verificato che i suoi dati sono corretti in anagrafica procede con la firma del documento di deposito dello specimen di firma e conferma le firme apposte con il tasto "Fatto". Il processo eseguito è il seguente ovvero Il SIGNificant Client propone un'immagine ottimizzata del pdf ricevuto dall'applicazione (pdf su cui il SIGNificant Server ha calcolato l'impronta "hash" del documento) e presenta il campo di firma, raccoglie i tratti grafici e biometrici del firmatario, mentre viene eseguita la firma, i dati raccolti sono cifrati nella memoria del dispositivo mobile con chiave simmetrica AES. Tale chiave è generata in modo casuale dal SIGNificant Client. Tal chiave viene a sua volta cifrata con chiave pubblica RSA:

Durante questa operazione il firmatario ha il completo ed esclusivo controllo del processo di firma attraverso le seguenti funzioni:

- Controllo della firma che appone direttamente su tablet con penna compatibile con schermi touch nell'apposito campo firma del documento di deposito dello specimen di firma;
- Conferma della firma apposta mediante la selezione del campo **FATTO**;
- Cancellazione del tratto grafico per la ripetizione della firma con la selezione del campo **RIPROVA**;
- Annullare l'operazione dei firma selezionando il campo **CANCELLA**.

Con la selezione del campo FATTO il firmatario conferma la firma apposta, Il SIGNificant Client invia i dati al SIGNificant Server.

Le firme sono raccolte in un documento che viene chiuso con un certificato a nome della società e inviato in archiviazione a norma e invita immagine, via e-mail all'Addetto all'attività di intermediazione. In caso di errore tutti i dati sono cancellati e si segnala di ripetere tutta la procedura dall'inizio.

13.2 DEPOSITO DELLE FIRME CLIENTE

Il processo di deposito dello specimen di firma è un processo preliminare che viene svolto dall'Addetto all'attività di intermediazione e dal cliente.

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. 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. Completata questa fase si può procedere a depositare lo specimen di firma del cliente. L'Addetto all'attività di intermediazione completa la procedura applicando la sua firma (in modalità Firma Grafometrica) al fine di garantire che l'operazione sia stata eseguita in sua presenza.

In dettaglio, l'Addetto, tramite il dispositivo mobile (Tablet iPad), si identifica al sistema della AFI ed esegue l'accesso al sistema informativo aziendale con le proprie credenziali.

Seleziona la funzione di deposito dello specimen di firma e inizia le operazioni.

Dopo avere verificato tutte le informazioni relative al cliente si procede con la raccolta delle firme. Il processo eseguito è il seguente:

Il SIGNificant Client propone un'immagine ottimizzata del pdf ricevuto dall'applicazione (pdf su cui il SIGNificant Server ha calcolato l'impronta "hash" del documento) e propone il campo di firma e raccoglie i tratti grafici e biometrici del firmatario, mentre viene eseguita la firma, i dati raccolti sono cifrati nella memoria del dispositivo mobile con chiave simmetrica AES. Tale chiave è generata in modo casuale dal SIGNificant Client. Tal chiave viene a sua volta cifrata con chiave pubblica RSA:

Durante questa operazione il firmatario ha il completo ed esclusivo controllo del processo di firma attraverso le seguenti funzioni:

- Controllo della firma che appone direttamente su tablet con penna compatibile con schermi touch nell'apposito campo firma del documento di deposito dello specimen di firma;
- Conferma della firma apposta mediante la selezione del campo **FATTO**;
- Cancellazione del tratto grafico per la ripetizione della firma con la selezione del campo **RIPROVA**;
- Annullare l'operazione della firma selezionando il campo **CANCELLA**.

Con la selezione del campo FATTO il firmatario conferma la firma apposta, Il SIGNificant Client invia i dati al SIGNificant Server e riprende a chiedere l'ulteriore firma.

Le firme sono raccolte nel documento di specimen di firma che viene chiuso con un certificato a nome della società e copia del suddetto documento viene inviata al cliente utilizzando l'indirizzo di mail comunicato dal cliente. In caso di errore o annullamento tutti i dati sono cancellati e si segnala di ripetere tutta la procedura dall'inizio.

Si evidenzia che la firma dell'Addetto all'attività di intermediazione a conclusione della fase di firma serve ad attestare che ha riconosciuto il cliente ed seguito direttamente il processo.

13.3 IL PROCESSO DI FIRMA

I SIGNificant Client e SIGNificant Server sono in grado di firmare documenti in formato PDF con firma autografa, 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 il dispositivo mobile, si identifica al sistema della AFI ed esegue l'accesso al sistema informativo del Gruppo Azimut con le proprie credenziali;
- L'Addetto all'attività di intermediazione compila, richiede o seleziona il documento che desidera far sottoscrivere al cliente;
- Viene quindi inviato al dispositivo mobile il documento PDF compilato da far sottoscrivere al cliente;
- Il SIGNificant Client inoltra il documento PDF 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 dispositivo mobile dell'Addetto all'attività di intermediazione che attiva il processo di firma per il firmatario.

Il firmatario 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;
- Firma con la penna compatibile con schermi touch sul display del tablet nell'apposita area di firma;
- (**FATTO**) confermare la firma apposta;
- (**RIPROVA**) cancellare il tratto grafico della firma per riscriverla;
- (**CANCELLA**) annullare l'inserimento della firma.

Mentre il sottoscrittore esegue la firma, i dati biometrici che lo caratterizzano 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 RSA (a chiavi asimmetriche).

Con la conferma (FATTO) da parte del firmatario il SIGNificant Client invia al SIGNificant Server, i dati biometrici cifrati, la chiave AES cifrata, il tratto grafico ed il tipo di tablet utilizzato. 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 tratto grafico 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.

L'Addetto all'attività di intermediazione appone la propria sottoscrizione mediante firma grafometrica in conclusione delle operazioni di acquisizione delle firme del cliente. Tale firma viene gestita con la medesima operatività illustrata per la firma del cliente. Dopo che tutte le firme sono state apposte l'utente conferma la conclusione della sottoscrizione del documento.

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 e-mail o nell'area riservata MyAzimut).

13.4 LE COMUNICAZIONI CIFRATE

La comunicazione ed il trasferimento dei dati biometrici 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 biometrici tra il Client ed il Server sono su un canale HTTPS (criptato) con algoritmo asimmetrico.

14 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.

14.1 CHIAVE PUBBLICA DI CIFRATURA

I dati biometrici 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.

14.2 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.

14.3 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.

14.4 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.

15 COMPONENTI DI SICUREZZA

15.1 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.

15.2 DEVICE

Nell'ambito del progetto Azimut ha deciso di adottare la soluzione AirWatch acquisendo il servizio da Magnetic Media Network.

MMN offre un servizio di Mobile Device Management tramite la piattaforma AirWatch, tramite la quale è possibile effettuare il controllo e la configurazione degli apparati ad uso della rete, la distribuzione di applicazioni e contenuti in modo sicuro ed efficiente.

- Il sistema è in grado di controllare apparati diversi in termini di sistemi operativi, in questo caso si prevede utilizzo solo di apparati iOS.
- Il servizio minimo comprende l'attivazione degli apparati e la configurazione di base degli stessi.
- Sono disponibili diverse interfacce di accesso al sistema che può essere utilizzato anche "as-a-service" da parte del personale della **AFI** o di **ObjectWay**.

In fase di rilascio degli apparati, viene effettuata la configurazione tramite un "profilo base" che prevede i seguenti parametri:

- Obbligo dell'uso di un PIN per lo sblocco dell'apparato.
- Blocco del backup e del trasferimento di dati "aziendali".

In particolare, per i device iOS i dispositivi saranno affidati, attraverso relativa procedura di iscrizione, al sistema *AirWatch* il quale si occuperà della loro gestione e controllo. Il sistema *AirWatch* effettua una verifica costante dei dispositivi per accertarne la conformità. Tale conformità prevede che lo stesso soddisfi determinate caratteristiche tra le quali:

- Codice di blocco presente.
- Memoria criptata.

La verifica di questi requisiti garantisce che il dispositivo, il sistema operativo e tutte le applicazioni in esso contenute siano originali e certificate. Garantisce che il dispositivo non sia utilizzabile se non attraverso il possesso del codice di sblocco.

E' altresì garantito che le applicazioni pubbliche (gratuite o a pagamento) possono essere installate esclusivamente dallo store di Apple. Mentre per quanto riguarda le applicazioni aziendali, non veicolate dallo store di Apple, garantisce che siano state firmate con un certificato enterprise valido prima di essere distribuite e installate.

In caso di furto, previa richiesta o accordo con **Azimut Financial Insurance S.p.A.**, la soluzione di MDM potrà effettuare la cancellazione remota parziale (solo dati aziendali) o totale (dati aziendali e personali).

I dati su dispositivi iOS (iPAD , iPhone) sono conservati all'interno del dispositivo in forma criptata, accessibile solo a fronte di sblocco tramite codice.

Il dispositivo è gestito attraverso AirWatch, grazie al quale è possibile, in caso di furto o smarrimento e a fronte di specifica richiesta o accordo, effettuare il Remote-Enterprise-WIPE ossia la cancellazione dei dati aziendali (configurazioni e applicazioni) dal dispositivo. Questa operazione è veicolata attraverso la connessione internet ed ha effetto immediato

L'utente ha sempre la facoltà di scollegare il dispositivo dal sistema MDM, attraverso la semplice rimozione di un profilo di configurazione. Tale pratica tuttavia rimuove tutte le configurazioni, le applicazioni aziendali e i dati rilasciati dall'azienda, rendendo di fatto il dispositivo inutilizzabile ai fini lavorativi.

16 ARCHIVIAZIONE E CONSERVAZIONE A NORMA DEI DOCUMENTI

Il processo di archiviazione, datacertazione 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:

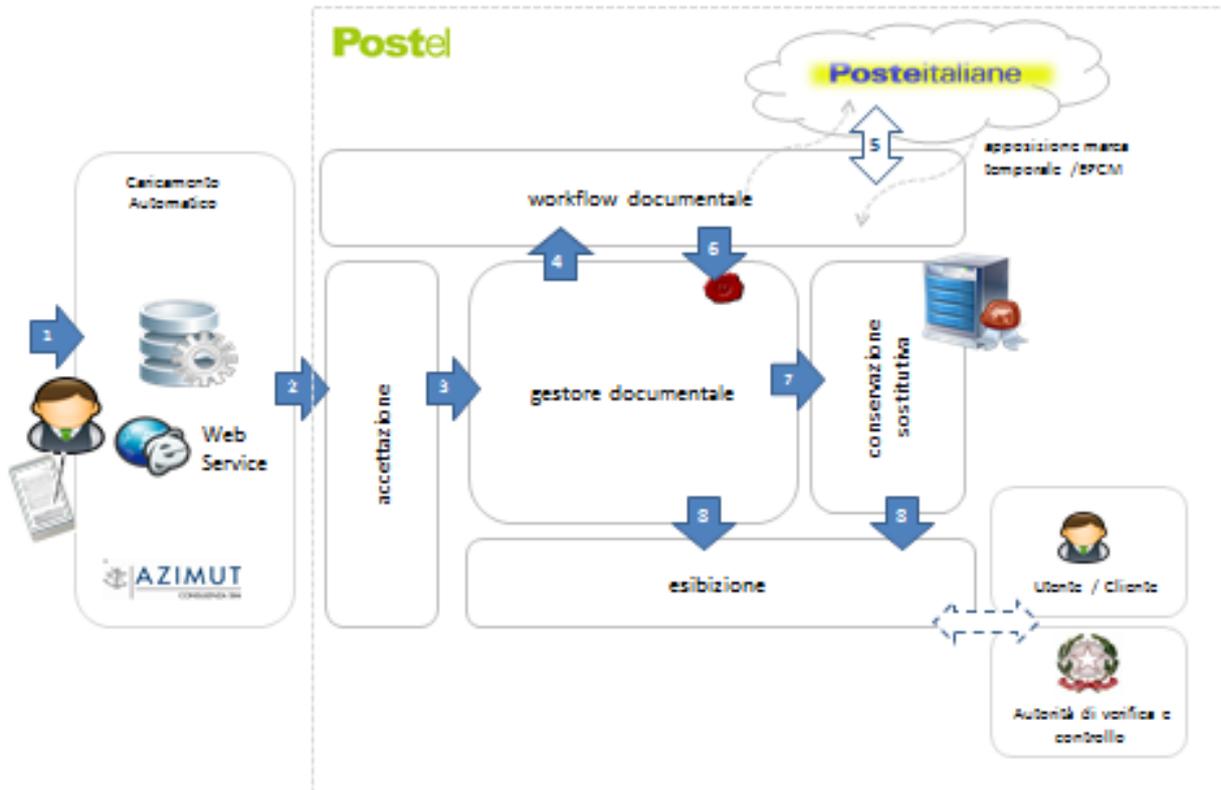
- Reverse Proxy IBM http Server 6.1, Apache web server (RP1),
- Data Server Oracle 10G in alta affidabilità (PB1, PB2),
- Content Serve con SO Red Hat Enterprise Linux 5.0 (CS1,CS2),
- Application Server con SO Red Hat Enterprise Linux 5.0 e Web Server IBM WS 6 (WS1, Ws2),
- Storage dati di tipo SAN (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 biometrici, 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)

17 LA GESTIONE DEL CONTENZIOSO

Il processo di gestione di un contenzioso, inizialmente segue le classiche politiche di gestione previste dall'istituto ma, in ipotesi che il contenzioso veda l'intervento di giudici per risolverlo, si deve obbligatoriamente prevedere un diverso approccio di perizia.

In particolare è necessario procedere ad una perizia dei dati informatici e biometrici delle firme in contenzioso.

Per questo motivo Xyzmo mette a disposizione un software che permette il confronto dei dati biometrici e informatici della firma nonché la visione 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 contestato e del documento di deposito degli specimen di firma;
- 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 fa apporre una nuova firma al cliente e la analizza confrontando i dati sia con il documento contestato sia con gli specimen di firma ed eventualmente con altri documenti firmati entro un periodo di un anno.