ALLEGATO n. 3
Interoperabilità dei sistemi di protocollo e la posta certificata

Premessa

Il presente documento propone, allo stato attuale della normativa e della tecnologia, alcune osservazione e linee guida verso l'interoperabilità dei sistemi di protocollo informatico. Il documento vuole essere una guida rapida e efficace per le persone operanti nelle pubbliche amministrazioni e che vogliano realizzare progetti che consentano lo scambio di documenti elettronici sia con altre amministrazioni sia con cittadini ed imprese. Tali progetti potranno basarsi su sistemi di protocollo informatico che siano fra loro interoperabili e su un'infrastruttura di posta elettronica certificata.

Quadro normativo

Dal punto di vista normativo il periodo 1999-2002 è stato caratterizzato da un'azione coordinata di interventi che definiscono un nuovo quadro di riferimento per la gestione elettronica delle attività amministrative:

- la Direttiva del Presidente del Consiglio dei Ministri 28 ottobre 1999, riguardante le gestione informatica dei flussi documentali nella Pubblica Amministrazione;
- le regole tecniche AIPA sul protocollo informatico approvate il 2 dicembre 1999;
- le regole tecniche riportate nel decreto del Presidente del Consiglio dei Ministri, 31 ottobre 2000, n. 272;
- la delibera AIPA n.51/2000 del 23 novembre 2000, recante regole tecniche in materia di formazione e conservazione di documenti informatici nelle pubbliche amministrazioni;
- la circolare AIPA/CR/28, del 7 maggio 2001, circa gli standard, modalità di trasmissione, formato e definizione dei tipi di informazioni minime ed accessorie comunemente scambiate tra le pubbliche amministrazioni e associate a documenti protocollati;
- la circolare AIPA/CR/31, del 21 giugno 2001, recante regole tecniche per il protocollo informatico;
- il Decreto del Presidente della Repubblica 28 dicembre 2000 n.445 - Testo Unico sulla Documentazione Amministrativa;
- la delibera AIPA n.42 del 13 dicembre 2001, recante le regole tecniche per la riproduzione e conservazione di documenti su supporto ottico;
- Il Decreto Legislativo 23 gennaio 2002 n.10 - riguardante il recepimento della direttiva 1999/93/CE sulla firma elettronica.

Quali funzionalità realizzare?

Il recente quadro normativo colloca il sistema di protocollo informatico in stretta relazione con altri sistemi quali: gestione dei documenti elettronici, sistema di archiviazione e conservazione dei documenti, strumenti per la garanzia di accesso agli atti amministrativi, controllo di gestione; tracciamento e esecuzione automatica dei flussi di lavoro (workflow).

Il protocollo "classico" (sistema di certificazione e registrazione della corrispondenza) va visto pertanto in stretta connessione con tutte le soluzioni tese al superamento del tradizionale scambio di informazioni cartacee

Sia nel caso della informatizzazione dei processi che nel caso della gestione documentale il livello di automazione da attuare nelle singole amministrazioni non può che essere determinato dalle stesse amministrazioni attraverso una analisi delle proprie esigenze rapportate alle opportunità di sviluppo offerte dalle recenti tecnologie.

Nel presente paragrafo si fornisce una schematizzazione dei possibili livelli realizzativi partendo dal cosiddetto "nucleo minimo" la cui realizzazione è obbligatoria per tutte le amministrazioni.

La prima attività da svolgere per una corretta riorganizzazione dei sistemi documentali elencati, consiste nell'individuazione, all'interno dell'amministrazione, delle *Aree organizzative Omogenee*, nel seguito AOO.
Una AOO può essere definita come un insieme di unità organizzative dell'amministrazione che usufruiscono, in modo omogeneo e coordinato, degli stessi servizi per la gestione dei flussi documentali. Una unità organizzativa associata ad una AOO è un utente dei servizi messi a disposizione dalla AOO stessa. Una AOO offre, in particolare, il servizio di protocollazione dei documenti in entrata ed in uscita che avviene utilizzando una unica sequenza numerica, rinnovata ad ogni anno solare, propria all'area stessa .

Per la determinazione dei confini delle AOO, in sede di analisi organizzativa e di valutazione di fattibilità delle soluzioni informatiche, andranno considerate le esigenze di certificazione dei documenti interni (inter e/o intra AOO) e andrà valutato se separare la certificazione del passaggio dei documenti a valenza esterna dal tracciamento dei passaggi dei documenti all'interno della struttura

Il nucleo base di un sistema di protocollo informatico presenta delle caratteristiche finalizzate a fornire almeno dei ***servizi di certificazione*** relativi alla ricezione di documenti ed alla loro formazione. Di fatto, la vigente normativa assume una forma molto dettagliata solo nel regolamentare le cosiddette operazioni di "registrazione" e "segnatura" di protocollo ovvero, in ultima analisi, le minime operazioni necessarie per la tenuta di un registro informatico che tiene traccia degli eventi di transito attraverso i confini dell'AOO dei documenti ufficiali, sia in ingresso che in uscita. Più specificamente, l'effettuazione di una "registrazione di protocollo" corrisponde alla assunzione delle seguenti responsabilità da parte dell'amministrazione:

1. *Certificare l'esistenza del documento almeno a partire da una certa data*. Questo significa che nel caso di documenti ricevuti, l'amministrazione non può negare, a fronte della richiesta di esibizione del contenuto di una registrazione, che un documento sia esistito. Similmente, nel caso di documenti prodotti dall'amministrazione, la stessa può "provare" che un proprio documento è stato formato ad una certa data.
2. Nel caso di documenti ricevuti, certificare il fatto che il documento è entrato nei confini dell'amministrazione e che subirà una qualche forma di trattamento.[1]

[1] Non necessariamente l'effettuazione di una registrazione protocollo corrisponde o corrisponderà all'avvio di un procedimento amministrativo.

I livelli realizzativi

Uno dei primi obiettivi che ciascuna amministrazione si deve dare nel definire un progetto di informatizzazione dei flussi documentali rispondente ai principi ed i requisiti fissati dalla normativa vigente, è quello di individuare il proprio "livello realizzativo", corrispondente alle funzionalità che essa stessa vuole realizzare.

In via indicativa, sono stati individuati quattro livelli di realizzazione del protocollo informatico - e quindi quattro diverse tipologie di intervento:

1. Nucleo minimo protocollo, che realizza le seguenti funzionalità:
   - registrazione in un archivio informatico delle informazioni riguardanti un documento (numero, data, mittente/destinatario, oggetto, ecc.);
   - segnatura sul documento delle informazioni riguardanti il documento stesso (numero, data, AOO);
   - classificazione d'archivio per una corretta organizzazione dei documenti
2. Gestione documentale, che realizza le seguenti funzionalità:
   - Registrazione con trattamento delle immagini e scannerizzazione dei documenti cartacei;
   - Assegnazione ai destinatari delle pratiche per via telematica
   - Collegamento dei documenti alla gestione dei procedimenti
   - Realizzazione di repository documentali
3. Workflow documentali, che realizza le seguenti funzionalità:
   - Informatizzazione dei processi relativi ai flussi documentali in entrata ed in uscita;
   - Informatizzazione dei processi relativi ai flussi documentali interni;
   - Integrazione con workflow
4. BPR, che realizza le seguenti funzionalità:
   - Riorganizzazione degli assetti organizzativi;
   - Creazione di sistemi di monitoraggio dei costi e dei tempi;
   - Integrazione i processi di pianificazione strategica e controllo di gestione

Come si può ben vedere, la scelta del tipo di intervento quindi ha ricadute in termini di complessità, di costi, di formazione, di ruoli coinvolti, ecc; ed ha una specifica valenza strategica nel momento in cui definisce e qualifica il progetto stesso:

Questa classificazione, a carattere ovviamente indicativo, deve essere letta con cautela. E' molto probabile, ad esempio, che nel momento in cui si decida di arrivare alla informatizzazione dei processi documentali (funzionalità 3), si sia già provveduto – o si intenda provvedere contestualmente – all'attivazione delle funzionalità 2, avviando

dapprima l'analisi organizzativa e in seguito lo studio del sistema informativo a supporto della razionalizzazione perseguita.

Nell'avviare un progetto di gestione elettronica dei documenti una volta definiti gli obiettivi relativi alle funzionalità da implementare - e quindi nella fase di scrittura del capitolato tecnico - le amministrazioni potranno fare riferimento ai documenti di progetto di altre amministrazioni che hanno già provveduto alla realizzazione di un tale sistema.

Come impostare l'architettura informatica?

Data la natura trasversale del processo di protocollazione rispetto ai processi primari di una amministrazione, è evidente come il problema della definizione della architettura del sistema di protocollo informatico sia strettamente correlato alla definizione dell'intero sistema informativo della amministrazione.

Nel presente capitolo si analizzeranno differenti soluzioni architetturali per la realizzazione del sistema di protocollo informatico e la loro collocazione rispetto all'architettura generale del sistema informatico dell'amministrazione.

Soluzione minima

C'è innanzitutto da distinguere tra il caso di realizzazione minima del sistema di protocollo informatico, ossia la esclusiva realizzazione delle essenziali funzioni di registrazione e classificazione e la realizzazione di funzioni più avanzate funzionali alla automazione dei flussi documentali delle amministrazioni. La realizzazione del solo "nucleo minimo" rappresenta una posizione nella quale il sistema di protocollo informatico può essere l'unico sistema automatizzato dell'area organizzativa omogenea che tratti in modo strutturato informazioni su documenti. In questo scenario è probabile che non esistano altri strumenti automatizzati, al di fuori del registro di protocollo e del sistema di classificazione (o eventuali strumenti di office automation), per trattare informazioni correlate alla gestione documentale (come, ad esempio, procedimenti e loro iter, oppure il funzionario responsabile, l'assegnatario, le scadenze ecc.).

Questo scenario è ipotizzabile nei casi in cui l'amministrazione o l'AOO tratti un volume estremamente basso di documenti, e quindi non sussistono le condizioni per rendere economicamente conveniente l'utilizzo di ulteriori strumenti informatici, oppure nel caso in cui ci siano vincoli sul grado di informatizzazione o il livello culturale informatico del personale.

Mentre l'ultima caso è auspicabilmente da superare, non è da considerarsi come condizione negativa la rinuncia all'utilizzo di ulteriori strumenti informatici per la gestione di informazioni sui documenti nel caso in cui il volume dei documenti trattati sia basso (ad esempio, non è detto che nel caso di un comune con 500 abitanti debba necessariamente avere un sistema di workflow per tenere traccia dello stato delle poche pratiche che il comune tratta ogni anno).

Se la scelta dell'amministrazione è di realizzare funzioni e servizi aggiuntivi rispetto al solo nucleo minimo si presentano diversi scenari e possibilità architetturali.

Soluzione monolitica

Un tipico scenario è quello in cui il sistema di protocollo venga realizzato fin dall'inizio come un sistema in grado di gestire, oltre ai dati necessari alla tenuta del registro di protocollo, anche tipi di informazioni legati al trattamento dei processi svolti dall'amministrazione, come "l'assegnatario della pratica", "il fascicolo" o "il procedimento amministrativo". In molti casi le amministrazioni adottano la soluzione di sviluppare una applicazione "ad hoc", monolitica, incentrata sul registro di protocollo, ma in grado di gestire un po' di tutto: il tracciamento delle pratiche attraverso forme più o meno sofisticate di workflow, alcune informazioni relative al controllo di gestione, una base dati documentale (usualmente limitata ai documenti protocollati con varie possibilità di accesso e ricerca).

Tipicamente all'interno di applicazioni di questo tipo si fa riferimento alle informazioni sulla struttura organizzativa dell'amministrazione, cioè dipendenti, ruoli, uffici unità organizzative ecc. Quindi all'interno dell'applicazione di protocollo si viene a creare una base dati (parziale o totale, bene aggiornata o male aggiornata) della struttura organizzativa. Inoltre nella applicazione si viene spesso a creare un elenco di corrispondenti, cioè una base dati di soggetti contenente nomi, indirizzi ed altre informazioni, che interagiscono a vario titolo con l'amministrazione.

Sia nel caso della struttura organizzativa e dei corrispondenti esterni, ma anche dei documenti, ci si trova di fronte ad una applicazione, cosiddetta di protocollo, ma che in realtà "invade" altri campi, cioè gestisce informazioni che rappresentano il patrimonio informativo dell'amministrazione indipendentemente dal fatto che siano collocate in un contesto di gestione documentale.

In alcune realtà tale tipo di soluzione potrebbe ancora risultare conveniente. Laddove, ad esempio, la amministrazione sia caratterizzata da una forte staticità (procedimenti ben identificati con iter stabili, carichi di lavoro prevedibili ecc.) allora potrebbe aver senso costruire una applicazione monolitica perfettamente ritagliata su tali esigenze che, per definizione, non variano. In generate, tuttavia, una soluzione di tipo monolitico rappresenta una *legacy* che impedisce un facile adattamento del sistema di gestione documentale alla variazione delle esigenze dell'amministrazione ed alla evoluzione delle tecnologie e dell'offerta del mercato informatico.

Soluzione modulare

Un ulteriore scenario, che rappresenta il modello più evoluto, è quello in cui il nucleo minimo del protocollo sia visto come un ***modulo applicativo,*** esclusivamente dedicato al servizio di certificazione, con tutte le caratteristiche previste dalla normativa e dalle regole tecniche. Il modulo di protocollo, piuttosto che fornire direttamente all'utente le funzioni di certificazione previste, diviene accessibile da parte di altre applicazioni, o componenti, che costituiscono il sistema informatico dell'amministrazione. In altre parole, il servizio di protocollo è un servizio richiamabile da altre parti (e quindi integrabile nei più vari contesti applicativi).

Nel contesto architetturale che si viene a delineare, oltre al servizio di certificazione di protocollo, dovrebbero essere messi a disposizione, centralmente a tutti i potenziali utilizzatori, altri servizi che costituiscono il patrimonio comune dell'amministrazione, secondo criteri opportuni di visibilità e sicurezza.

Scenari intermedi

Ogni forma intermedia di configurazione tra lo scenario monolitico e quello modulare è ovviamente possibile, anzi è probabile che la maggioranza delle applicazioni esistenti ricada in questa categoria. A meno di applicazioni monolitiche basate su tecnologie proprietarie (ad esempio sistemi basati su mainframe) ogni soluzione che comporti l'uso di tecnologie di supporto aperte di tipo client/server, facenti uso di strumenti ed ambienti di mercato, offre una qualche forma di modularità e di accessibilità.

La soluzione più ricorrente è quella di incentrare il sistema di gestione del protocollo e delle pratiche su un ***database*** e offrire a vari profili client la possibilità di attivare diverse operazioni sul sistema. Su questi sistemi è possibile operare degli interventi tesi ad incrementare la modularità e l'indipendenza tra i vari componenti, fino ad arrivare ad una eventuale sostituzione di alcune funzioni. Le tecniche di *wrapping* e l'utilizzo di middleware specifico possono risultare di ausilio a queste iniziative di riconversione.

Stabilire se è conveniente per una amministrazione avviare un programma di "modularizzazione" di un sistema di gestione documentale e di protocollo informatico è

comunque una decisione che dovrà scaturire da una attenta valutazione dei costi e dei benefici dell'operazione.

Interoperabilità dei sistemi di protocollo

La Circolare AIPA del 7 maggio 2001 AIPA/CR/28 recepisce le indicazioni presenti nel Testo Unico sulla documentazione amministrativa in materia trasmissione di documenti in formato elettronico fra pubbliche amministrazioni, e fornisce le regole tecniche per l'interoperabilità dei sistemi di protocollo, ossia per il "trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente, allo scopo di automatizzare altresì le attività ed i processi amministrativi conseguenti"

Precedentemente alla circolare citata, il DPCM 31 ottobre 2000 n.272 ha stabilito le modalità comuni di comunicazione fra le pubbliche amministrazioni atte a consentire una corretta trasmissione di documenti elettronici. Tale decreto ha anche stabilito che lo strumento con cui effettuare la trasmissione telematica dei documenti è la **posta elettronica basata su SMTP/MIME[2]**. Inoltre, per facilitare le operazioni di trasmissione dei documenti informatici, il decreto ha istituito **l'indice delle amministrazioni pubbliche e delle aree organizzative omogenee**, gestito tramite un sistema informatico, accessibile mediante un sito internet, e compatibile con il protocollo LDAP. Ogni amministrazione, che intenda trasmettere documenti in formato elettronico, deve registrarsi presso l'indice, fornendo le seguenti informazioni:

- denominazione dell'amministrazione;
- codice identificativo;
- indirizzo della sede principale;
- elenco delle proprie AOO.

A loro volta, le AOO di un'amministrazione registrata devono rendere disponibili, nell'indice le seguenti informazioni:

- denominazione;
- codice identificativo;
- casella di posta elettronica, adibita alla protocollazione dei messaggi ricevuti;
- nominativo del responsabile del servizio di tenuta del protocollo informatico;
- data di istituzione;
- eventuale data di soppressione;
- elenco degli uffici afferenti alla AOO.

Lo scambio di documenti in formato elettronico fra pubbliche amministrazioni deve avvenire utilizzando la casella di posta elettronica dell'AOO destinataria del messaggio e deve corrispondere ad un'operazione di registrazione di protocollo, che può riguardare sia il corpo del messaggio che gli eventuali file ad esso allegati.

Le informazioni relative alla segnatura di protocollo dei documenti trasmessi devono essere codificate dall'amministrazione mittente in formato XML, secondo la DTD (Document Type Definition) stabilita nella circolare AIPA sopraccitata, e devono essere inserite in una body part[3] del messaggio di posta denominata Segnatura.xml. Le informazioni da includere nella segnatura di protocollo del messaggio sono, al minimo:

- oggetto;
- mittente;
- destinatari

L'amministrazione destinataria protocolla il messaggio ricevuto, utilizzando per la registrazione le informazioni contenute nella segnatura informatica.

[2] Per le amministrazioni che hanno sottoscritto il contratto di interoperabilità della RUPA il servizio di posta elettronica è quello offerto dal fornitore del servizio.

[3] Secondo lo standard MIME un messaggio di posta elettronica è composto da diverse parti (body part) identificate, all'interno della struttura del messaggio stesso, da un nome univoco.

Accanto ai messaggi di posta elettronica protocollati in ingresso ed in uscita dalle amministrazioni riceventi e mittenti, la normativa ha identificato un'altra tipologia di messaggi, detti **messaggi di ritorno**. Tali messaggi, codificati secondo lo stesso standard MIME e scambiati attraverso SMTP, hanno lo scopo di comunicare eventi ed informazioni alle diverse AOO coinvolte. I messaggi di ritorno si dividono in:

- messaggi di conferma di ricezione;
- messaggi di notifica di eccezione;
- messaggi di aggiornamento di conferma;
- messaggi di annullamento di protocollazione.

Rimandando alla circolare AIPA del 7 maggio 2001 per la descrizione di dettaglio dei messaggi di ritorno, si sottolinea che il loro uso è particolarmente interessante per quelle amministrazioni che si volessero dotare di un servizio di posta elettronica certificata.

La posta elettronica certificata

Il Testo Unico sulla documentazione amministrativa (DPR 445/2000) afferma l'equivalenza tra trasmissione telematica di documenti informatici e trasmissione per mezzo della posta tradizionale, purché siano utilizzati strumenti che assicurino l'avvenuta consegna dei messaggi.
Con il termine posta elettronica certificata si intende fare riferimento a tutti gli strumenti attraverso cui il normale servizio di posta elettronica SMTP/MIME diventi giuridicamente equivalente al servizio di posta tradizionale. Tali strumenti comprendono:

- la possibilità di firmare elettronicamente il messaggio;
- la possibilità di risalire, in modo inequivocabile, alla data ed all'ora di trasmissione([4]);
- la garanzia dell'avvenuta consegna all'indirizzo di posta elettronica dichiarato dal destinatario;
- l'adesione agli standard previsti per la Rete Nazionale e per l'interoperabilità e la cooperazione applicativa.

Modalità di interazione

Rispetto alla posta certificata, si possono evidenziare tre modalità di interazione:

- Scambio di messaggi e di allegati ordinari **tra individui**

Secondo questa modalità minimale un cittadino è in grado di inviare per posta elettronica ciò che presenterebbe altrimenti ad uno sportello (ad esempio un modulo compilato e firmato), con la garanzia che il relativo procedimento potrà venire avviato in modo del tutto analogo. L'impiegato che riceve la domanda o la documentazione dovrà naturalmente inserire manualmente nei sistemi informatici del dominio destinatario tutte le informazioni richieste dal procedimento.

- Scambio di messaggi e di allegati strutturati in XML **tra un individuo e un sistema informatico**

Questa modalità fa riferimento al caso in cui un individuo ricorra ai servizi a valore aggiunto erogati da un portale per inviare documenti strutturati (ad esempio moduli compilati). Il dominio destinatario è in grado di elaborare automaticamente la richiesta instradandola al sistema informatico interessato e realizzando così una forma blanda di integrazione applicativa tra portale e dominio dell'amministrazione. Un caso particolare di integrazione è quella con il sistema di protocollo informatico, che potrebbe ad esempio restituire al cittadino, per mezzo dello stesso canale di posta certificata ed in modo automatico, le informazioni riguardanti lo stato del procedimento.

[4] E' opportuno ribadire che i dati contenuti nell'intestazione SMTP di un messaggio, quali ad esempio la data e l'ora di invio, non sono rilevanti ai fini del trattamento amministrativo, valendo esclusivamente le informazioni riportate nella segnatura.

- Scambio di messaggi e di allegati strutturati in XML **tra sistemi informatici**

Questa modalità più avanzata è in verità del tutto analoga a quella che ha ispirato le modalità di integrazione applicativa basate sul protocollo SMTP e sulla busta di e-government, già descritte nelle linee guida sulla cooperazione applicativa.

Obiettivo di un'architettura di posta certificata

Lo scenario e le modalità di interazioni descritte sopra permettono di definire gli obiettivi di un'architettura di posta certificata, analizzata nel seguito. Accanto ai componenti principali di un sistema di posta elettronica insituzionale, le cui caratteristiche principali saranno evidentemente l'apertura e l'interoperabilità, sarà necessario definire standard e politiche di gestione che permettano al mercato dei servizi di posta certificata di svilupparsi in modo coerente con gli obiettivi di e-government. Tali standard potranno affrontare i temi dell'autenticazione del mittente e del destinatario e del non ripudio delle comunicazioni, ma anche quelli delle reti SMTP in termini di gestione dei server di posta, dei log e dei metodi di mutua autenticazione tra server.

L'assenza di regole tecniche che governino in modo esplicito la validità legale della posta elettronica non può essere considerata un ostacolo al suo utilizzo. È infatti sempre più diffusa la convinzione che la normativa sulla firma elettronica e il protocollo informatico, e il quadro rappresentato principalmente dal Testo Unico sulla documentazione amminstrativa, rappresentino una base normativa sufficente ad un uso esteso della posta certificata.

L'analisi dell'insieme di norme che regolano la gestione e lo scambio di documenti elettronici nelle pubbliche amministrazioni, oltre alle finalità legate all'e-government esposte sopra, inducono a definire un sistema di posta certificata che risponda ai requisiti illustrati di seguito:

- elevata garanzia di recapito
- opponibilità di fronte a terzi della provenienza e del recapito del messaggio
- trasparenza rispetto alla natura del messaggio (il messaggio può essere firmato o meno, protocollato o meno, crittografato o meno)
- possibilità di utilizzo con qualsiasi client di posta elettronica

In queste linee guida si definisce innanzitutto l'insieme di caratteristiche minimo che tutti i servizi di posta certificata devono obbligatoriamente presentare e quindi si individuano gli strumenti che possono permettere alle singole Amministrazioni di estendere ulteriormente le loro caratteristiche.

Un servizio di posta certificata che presenta l'insieme di caratteristiche minimo verrà detto "servizio di posta certificata di base"; un servizio di posta certificata che presenta, oltre alla caratteristiche minime obbligatorie anche quelle accessorie, verrà detto "servizio di posta certificata avanzato".

Modello architetturale

In questo capitolo si descrive il modello architetturale alla base di un sistema di posta certificata. Saranno precisate le definizioni necessarie e definiti gli scenari di utilizzo di tale servizio.

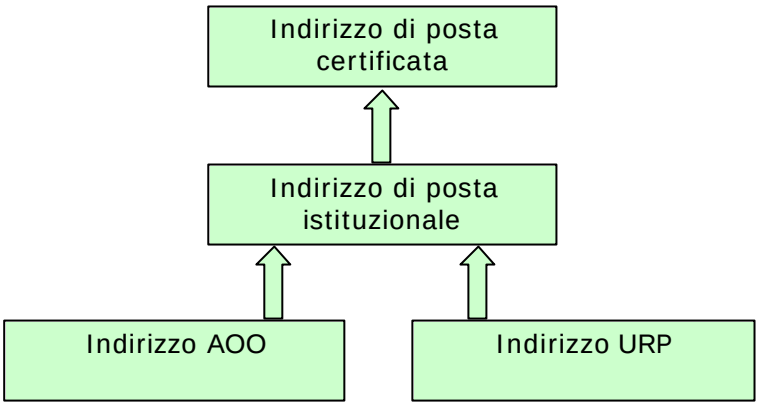
Definizioni

È possibile distinguere le seguenti tipologie di indirizzi di posta elettronica.

- Indirizzo di posta certificata: indirizzo di posta elettronica attraverso il quale è possibile accedere a servizi di posta certificata, ossia, un indirizzo di posta elettronica attestato su un servizio di posta certificata

– Indirizzo di posta istituzionale: un indirizzo di posta "dichiarato" da una Amministrazione in conformità all'art. 14 del Testo Unico. Esso è pubblicato dall'Amministrazione in un apposito indice e presumibilmente anche per altre vie, ed è per definizione "certificato".

Lo schema mostra, come esempi di possibili indirizzi di posta istituzionali, gli indirizzi delle AOO e degli URP.



Servizi accessori: servizio di directory

Un servizio di directory è necessario ai sistemi di posta certificata per rendere disponibili le informazioni sugli indirizzi di posta istituzionale dichiarati dalle Amministrazioni e per verificare le firme dei server di posta; un analogo servizio di directory è peraltro previsto dal regolamento tecnico del protocollo informatico (DPCM 31 ottobre 2000, art. 11).

La descrizione approfondita e puntuale del servizio di directory esula dallo scopo di questo documento; si sottolinea soltanto il fatto che esso deve pubblicare almeno le seguenti informazioni:

– denominazione della Pubblica Amministrazione
– denominazione della casella di posta istituzionale
– indirizzo della casella di posta istituzionale
– certificato associato alla casella di posta istituzionale

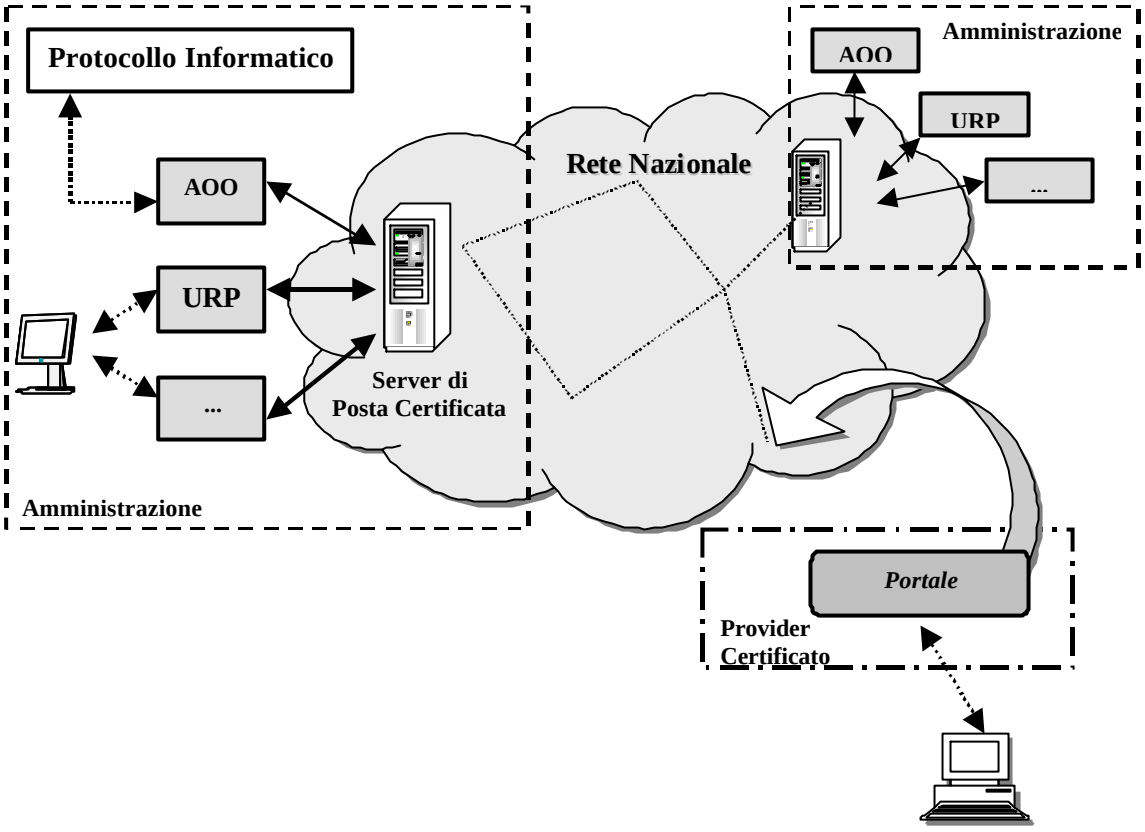
Attori

E' possibile identificare le seguenti tipologie di attori:

– **le amministrazioni** (enti centrali, territoriali e locali); nello scenario prefigurato esse utilizzano un servizio di posta certificata per lo scambio di documenti
– **gli intermediari** tra amministrazioni e soggetti privati, ossia dei provider che mettono a disposizione strumenti per accedere a un servizio di posta certificata; nel seguito del documento si supporrà che il servizio sia reso fruibile attraverso un portale
– **i cittadini e le imprese**, e più in generale tutti i soggetti che possono richiedere servizi alle amministrazioni; questi possono utilizzare i servizi di posta certificata messi a disposizione da intermediari per scambiare documenti con le pubbliche amministrazioni

Architettura di riferimento

I componenti architetturali che definiscono lo scenario di utilizzo di un sistema di posta certificata sono schematizzati nella figura seguente.



Le Amministrazioni si scambiano messaggi di posta certificata utilizzando la Rete Nazionale. I messaggi sono recapitati presso le caselle di posta certificata e quindi acceduti dai destinatari finali; sono schematizzati gli indirizzi di posta elettronica certificata già citati precedentemente.

Lo schema illustra degli esempi di come, all'interno di una Amministrazione, i messaggi di posta certificata possono essere utilizzati:

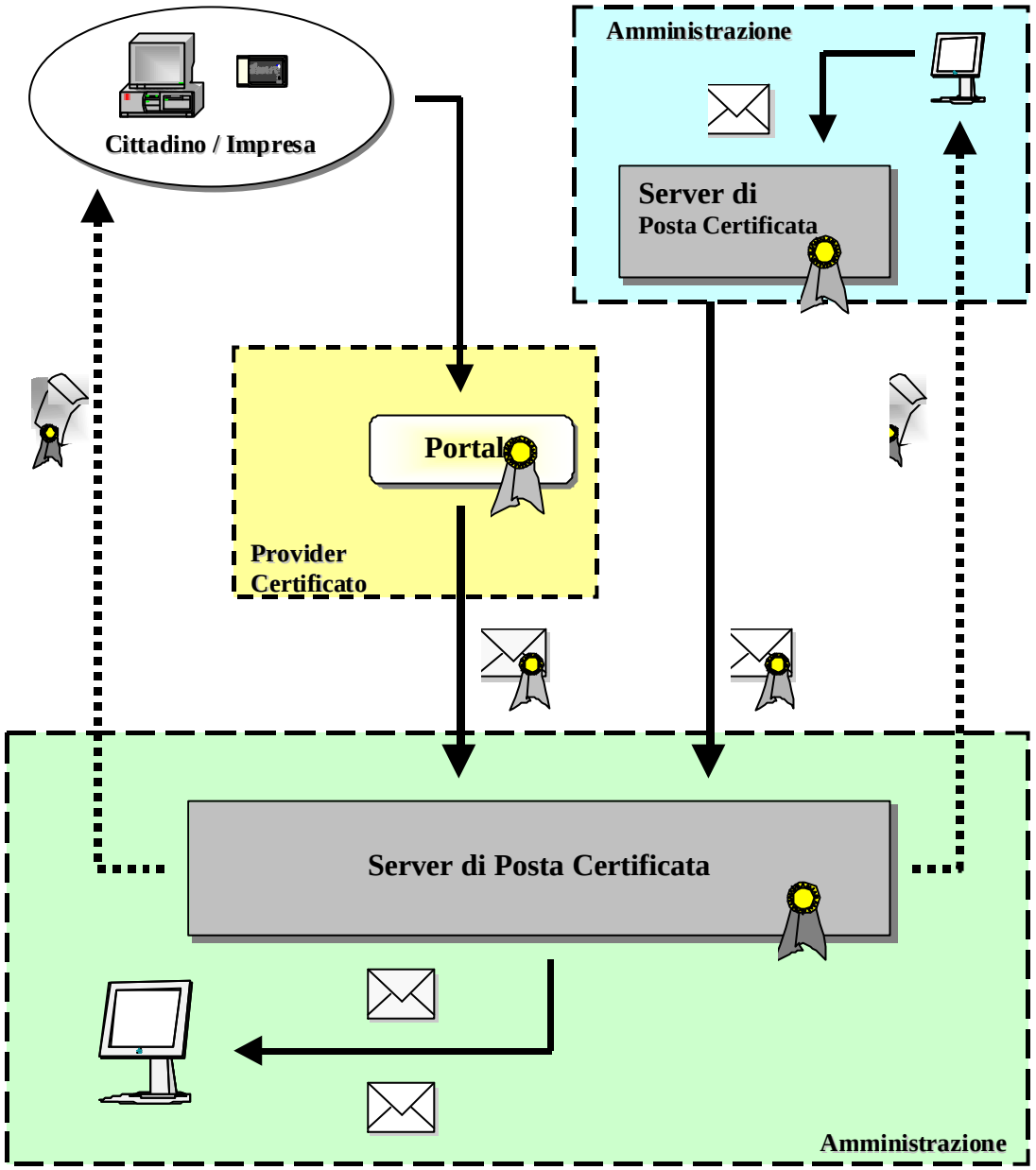
- una applicazione di Protocollo Informatico che accede alla casella istituzionale della corrispondente AOO
- altre applicazioni o funzionari che accedono ognuno alle caselle istituzionali di competenza.

Gli interlocutori che non appartengono a una pubblica amministrazione possono utilizzare i servizi messi a disposizione da terze parti. Questi servizi dovranno presentare le stesse caratteristiche e rispondere agli stessi requisiti previsti per le pubbliche amministrazioni; essi potranno essere resi fruibili con le modalità e le politiche che il provider riterrà opportune.

Lo schema delineato non preclude il fatto che gli interlocutori che non appartengono a una pubblica amministrazione possano utilizzare i tradizionali servizi di posta elettronica, indirizzando i messaggi a un indirizzo di posta dichiarato da una amministrazione. E' evidente però come non si possa parlare in questo caso di messaggi di posta certificata in quanto questo meccanismo non garantisce il rispetto di tutte le caratteristiche indicate in precedenza. In particolare, anche se i server di posta certificata invieranno comunque una ricevuta di ritorno, risulta impossibile garantire il mittente sulla non ripudiabilità del messaggio che egli ha spedito.

Tipologia dei messaggi scambiati

Il tipo di messaggi che transitano all'interno di un servizio di posta certificata sono evidenziati nel diagramma seguente.



In una amministrazione, il funzionario prepara e invia il messaggio, che viene quindi preso in carico dal server di posta certificata dell'amministrazione; il server, in maniera automatica, calcola il Message Authentication Code (MAC) utilizzando la propria chiave privata e lo appone al messaggio: in questo modo sarà possibile al server destinatario controllare l'identità del server mittente.

Il messaggio così certificato viene recapitato al server di posta certificata destinatario; quest'ultimo autentica il server mittente, sfruttando il MAC apposto al messaggio, e lo recapita al destinatario finale. Contestualmente, il server di posta certificata destinatario produce il messaggio di ricevuta di ritorno e lo spedisce al mittente: anche questo, come il messaggio originario, viene certificato dal server che lo invia, calcolando e apponendo il MAC; in questo modo, il server mittente del messaggio originario è garantito sul fatto che esso è stato recapitato correttamente.

Il diagramma evidenzia anche il flusso che si origina quando il messaggio è spedito da un interlocutore esterno a una pubblica amministrazione; si fa l'ipotesi che il mittente sia in grado di sottoscrivere con firma digitale il documento informatico che intende inviare, così da dotarlo di efficacia probatoria.

I servizi di posta certificata sono in questo caso erogati da un provider certificato: è quindi responsabilità di quest'ultimo calcolare il MAC e apporlo al messaggio dell'utente.

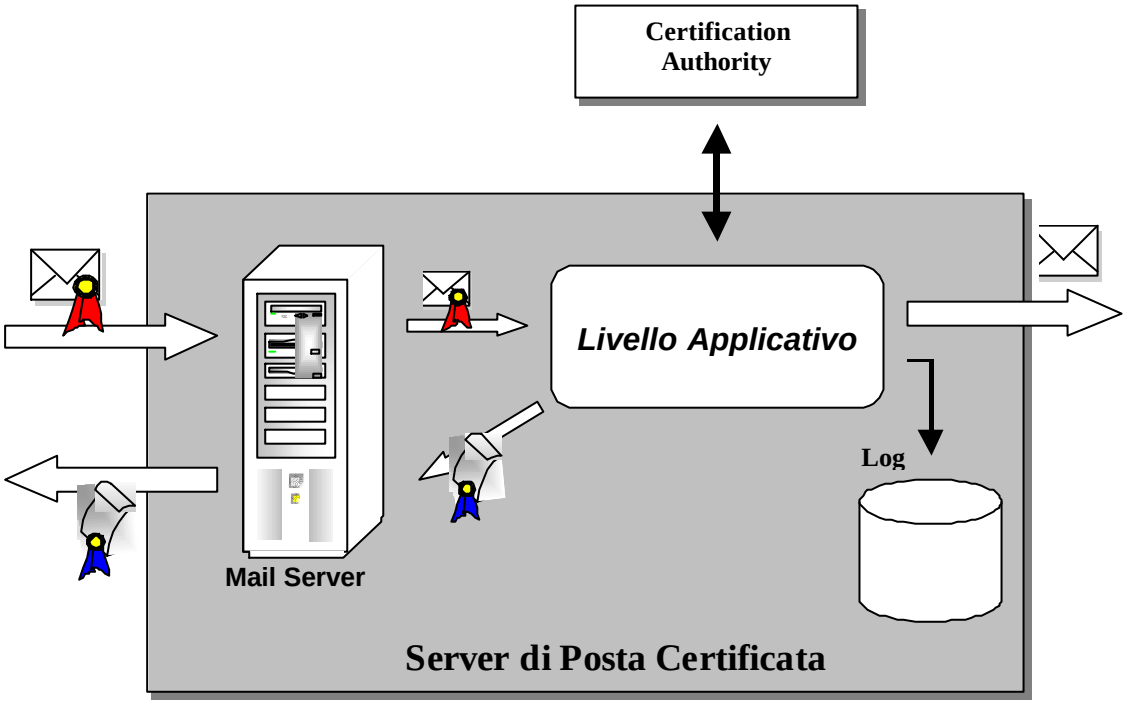
Architettura del server di posta certificata

Un server di posta certificata deve quindi svolgere delle operazioni aggiuntive rispetto a un server SMTP tradizionale:

- accesso alle Certification Authority per la verifica dei MAC presenti sui messaggi ricevuti
- tracciamento delle attività nel Log di posta
- gestione automatica delle ricevute di ritorno

Queste attività sono svolte da uno strato applicativo dedicato.

Uno schema di massima dell'architettura è mostrato nella figura seguente, che evidenzia come questo strato applicativo interagisce con il mail server e con le Certification Authority durante la ricezione di un messaggio.



L'architettura illustrata si adatta alle diverse soluzioni proposte dal mercato ed è suscettibile di ulteriori estensioni da parte delle singole amministrazioni o dei provider certificati; si possono citare, ad esempio, la realizzazione di funzionalità avanzate per il disaster recovery e per le operazioni di backup dei messaggi e del Log di posta.

Ogni sistema dedicato può inoltre implementare al proprio interno meccanismi di consegna di messaggi differenziati:

- trasmissione diretta di messaggi al destinatario
- inoltro della sola notifica di presenza di un messaggio su un repository, con richiesta di accesso da parte dell'utente

Ipotesi progettuali

In questo capitolo vengono descritti alcuni possibili scenari operativi. Si assume che tutte la Amministrazioni siano dotate di servizi di posta certificata; si noti infatti che nel transitorio, ossia nel periodo in cui non tutte le Amministrazioni saranno dotate di questo servizio, il ruolo svolto da una Amministrazione non dotata del servizio è assimilabile a quello di un privato o di un azienda.

Gli attori coinvolti nei processi considerati sono:

- cittadino/impresa: è un attore che invia o riceve un messaggio a una PA, eventualmente per tramite di un provider certificato
- Pubblica Amministrazione (mittente e destinataria); è un attore che invia o riceve un messaggio a un'altra PA o a un cittadino/impresa
- Sistema di posta certificata (mittente e destinatario); esso può essere di base o avanzato
- Server di posta elettronica tradizionale
- Sistema di Protocollo Informatico (mittente e destinatario)

Caratteristiche di un servizio di base

L'insieme minimo di caratteristiche da prevedere deve essere tale da garantire il soddisfacimento dei requisiti posti e da poter essere realizzato con interventi leggeri sui server di posta attualmente disponibili.

Un servizio di posta certificata di base potrà quindi operare secondo le modalità seguenti, in aggiunta alle operazioni svolte da un servizio di posta tradizionale.

In fase di spedizione di un messaggio:

- aggiorna il Log di posta, per mantenere traccia della presa in carico del messaggio
- associa al messaggio da spedire il Message Authentication Code (MAC) calcolato utilizzando la propria chiave privata
- spedisce il messaggio, allegando il MAC e il proprio certificato

In fase di ricezione di un messaggio:

- aggiorna il Log di posta, per mantenere traccia della ricezione del messaggio
- autentica il messaggio ricevuto, ossia verifica l'identità del server mittente: il MAC e il certificato dal server mittente sono eliminati dal messaggio e salvati nel Log di posta;

a) se si verifica un errore, il server risponde con una ricevuta di ritorno di base che contiene nel body un messaggio standard di errore,

b) altrimenti esegue le operazioni seguenti

- verifica se il messaggio ricevuto è un messaggio di ricevuta di ritorno; i messaggi di ricevuta di ritorno sono identificati da un subject che inizia con la stringa standard "Ricevuta di ritorno di posta certificata"; in caso positivo non deve essere messa in atto nessuna operazione; in caso negativo il servizio calcola il MAC relativo al messaggio originario e produce un messaggio di ricevuta di ritorno da spedire al mittente (ricevuta di ritorno di base) con un messaggio standard di avvenuta ricezione

Le operazioni di autenticazione previste permettono ai server interlocutori di riconoscersi a vicenda.

La ricevuta di ritorno di base

Presenta le seguenti caratteristiche:

- è un messaggio SMTP spedito all'indirizzo di posta mittente
- il subject deve iniziare con la stringa standard "Ricevuta di ritorno di posta certificata", per consentire al server che ha spedito il messaggio originario di riconoscerlo come tale
- il body contiene un messaggio standard, di avvenuta ricezione o di errore
- contiene il messaggio originario; è questo il meccanismo più semplice per permettere al mittente di associare la ricevuta di ritorno al messaggio originante cui essa si riferisce

- contiene in allegato il MAC apposto sul messaggio originario e il certificato del server ricevente; questo per identificare il server che ha gestito il messaggio

Caratteristiche di un servizio avanzato

Questa sezione del documento dettaglia le estensioni che possono essere implementate al fine di ottenere un servizio di posta certificata più aderente alle necessità delle singole Amministrazioni.

Due sono le necessità individuate.

- In determinati contesti, un messaggio di posta elettronica può avere uno scopo diverso da quello della spedizione di un documento; si pensi ai messaggi di conferma di ricezione da parte di un sistema di Protocollo Informatico. In questi casi, la casella di posta è utilizzata come una porta applicativa.
- A seconda dell'ambiente operativo del server di posta certificata, l'associazione tra messaggio inviato e ricevuta di ritorno può essere mantenuta con meccanismi diversi

Per rispondere a queste necessità, oltre a garantire le funzionalità di un servizio di base, si prevede la possibilità di associare ai messaggi originari e ai messaggi di ricevuta di ritorno un allegato in formato XML che permetta di specificare le informazioni necessarie. Analogamente a quanto previsto nelle regole del Protocollo Informatico, anche il DTD minimo pubblicato dal Centro Tecnico potrà essere esteso, di comune accordo, da due o più Amministrazioni.

Il file XML da allegare al messaggio originario deve avere come nome "PostaCertificata.xml".

Il file XML da allegare al messaggio di ricevuta di ritorno deve avere come nome "RicevutaRitorno.xml".

Poiché il file "PostaCertificata.xml" ha lo scopo di indicare al server di posta certificata destinatario le operazioni che deve mettere in atto al momento della ricezione, è evidente come esso debba essere creato direttamente dal mittente (operatore o applicazione), in quanto è l'unico attore che può decidere quali devono essere queste operazioni.

Un Servizio di Posta Certificato Avanzato deve quindi operare secondo le modalità seguenti, in aggiunta alle operazioni svolte da un servizio di posta tradizionale.

In fase di spedizione di un messaggio:

- aggiorna il Log di posta, per mantenere traccia della presa in carico del messaggio
- calcola il MAC del messaggio da spedire
- spedisce il messaggio, allegando il MAC e il proprio certificato

In fase di ricezione di un messaggio:

- aggiorna il Log di posta, per mantenere traccia della ricezione del messaggio
- autentica il messaggio ricevuto, ossia verifica l'identità del server mittente; il MAC e il certificato dal server mittente sono eliminati dal messaggio e salvati nel Log di posta; se si verifica un errore, il server risponde con una ricevuta di ritorno di base che contiene nel body un messaggio standard di errore, altrimenti vengono eseguite le operazioni seguenti
  - verifica se il messaggio ricevuto è un messaggio di ricevuta di ritorno; i messaggi di ricevuta di ritorno sono identificati da un subject che inizia con la stringa standard "Ricevuta di ritorno di posta certificata"; in caso positivo non deve essere messa in atto nessuna operazione; in caso negativo il servizio firma il messaggio originario e:
    1) se il messaggio ricevuto contiene un allegato di nome "PostaCertificata.xml", il servizio elimina l'allegato dal messaggio, lo interpreta e opera secondo quanto indicato dal mittente, creando e spedendo, qualora richiesto, un messaggio di ricevuta di ritorno

2) se il messaggio contiene un allegato di nome "PostaCertificata.xml" ma il server avanzato non riesce a interpretarlo correttamente, esso invia un messaggio di ricevuta di ritorno in un formato standard e contenente una stringa che evidenzi l'errore riscontrato

3) se il messaggio non contiene un allegato di nome "PostaCertificata.xml", il server avanzato spedisce una ricevuta di ritorno di base

Formato dei messaggi

Il messaggio originario presenta le seguenti caratteristiche:

– è il messaggio SMTP spedito dal mittente a cui vengono allegati il MAC apposto sul messaggio e il certificato del server

Il messaggio originario creato da un utente che utilizza un servizio di posta certificata Avanzato può avere come allegato il file XML "PostaCertificata.xml"; esso contiene:

– indicazione se spedire la ricevuta di ritorno o se omettere tale spedizione

– nel caso di richiesta della ricevuta di ritorno, il meccanismo desiderato di identificazione del riferimento mittente, da scegliere nel seguente insieme predefinito: intero messaggio in "reply", impronta del messaggio da inserire in allegato (indicando anche il nome dell'allegato), indicazione di un riferimento alfanumerico in allegato (indicando anche il nome dell'allegato)

– nel caso di richiesta della ricevuta di ritorno, l'indirizzo di posta elettronica al quale spedirla se diverso dal proprio

– nel caso di richiesta della ricevuta di ritorno, la richiesta di eventuali time-stamp certificati relativi alla spedizione e alla ricezione del messaggio

Il messaggio di ricevuta di ritorno avanzata presenta le seguenti caratteristiche:

– è un messaggio SMTP spedito all'indirizzo di posta mittente

– il subject deve iniziare con la stringa standard "Ricevuta di ritorno di posta certificata", per consentire al server che ha spedito il messaggio originario di riconoscerlo come tale

– il body contiene un messaggio standard, di avvenuta ricezione o di errore

– contiene in allegato il MAC apposto sul messaggio originario e il certificato del server

– contiene in allegato il file "RicevutaRitorno.xml" che contiene informazioni di servizio

– l'informazione per permettere al mittente di associare la ricevuta di ritorno al messaggio originante cui essa si riferisce, specificata con il meccanismo indicato dal mittente

Il file "RicevutaRitorno.xml" contiene:

a) un insieme di informazioni generali

b) informazione necessaria ad associare la ricevuta al messaggi originario nel formato richiesto

c) messaggio di errore (opzionale)

Tra le informazioni generali, comunque facoltative, il file XML potrebbe contenere anche un insieme di informazioni già presenti nella struttura MIME, ma che possono essere replicati per una maggiore sicurezza e facilità di utilizzo da parte di sistemi automatizzati; ad esempio

– indirizzo di posta originario

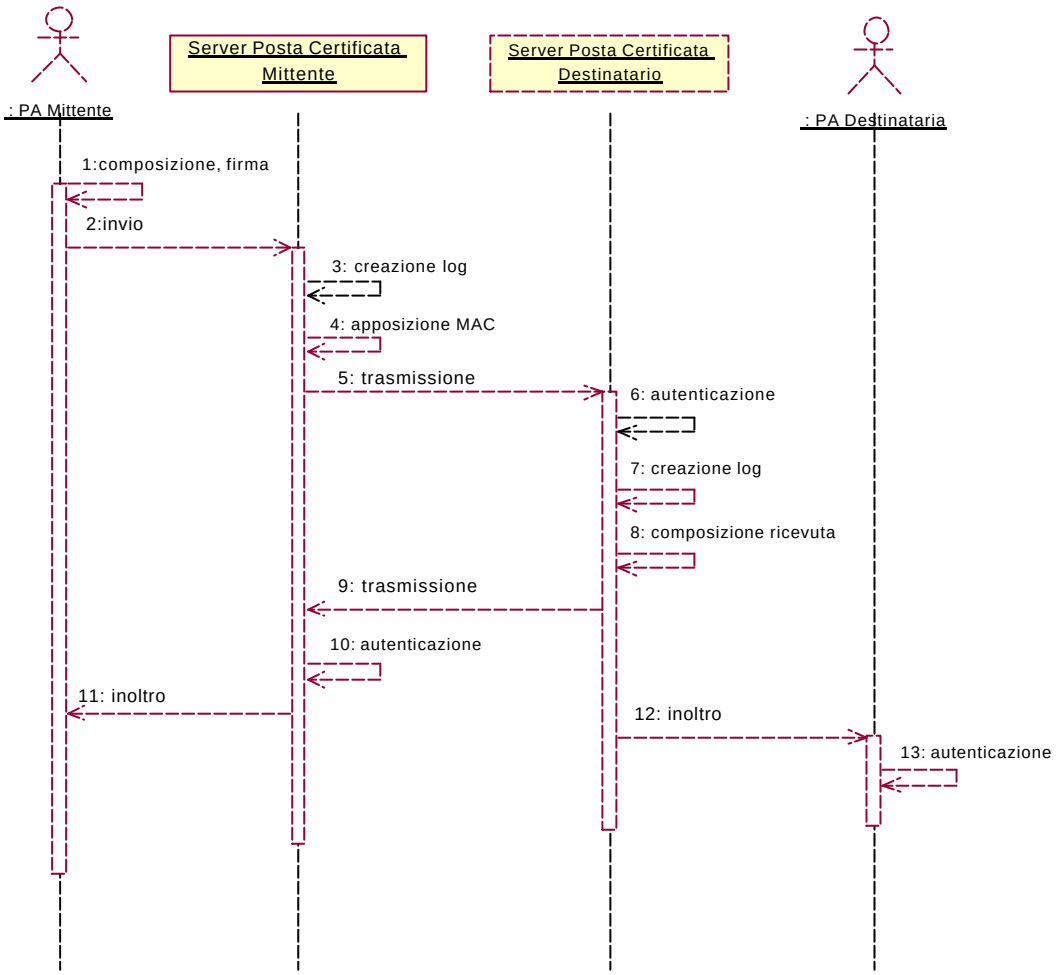
– indirizzo di posta destinatario

– data e ora di spedizione e di ricezione

Interazioni

Interazioni per messaggi non protocollati

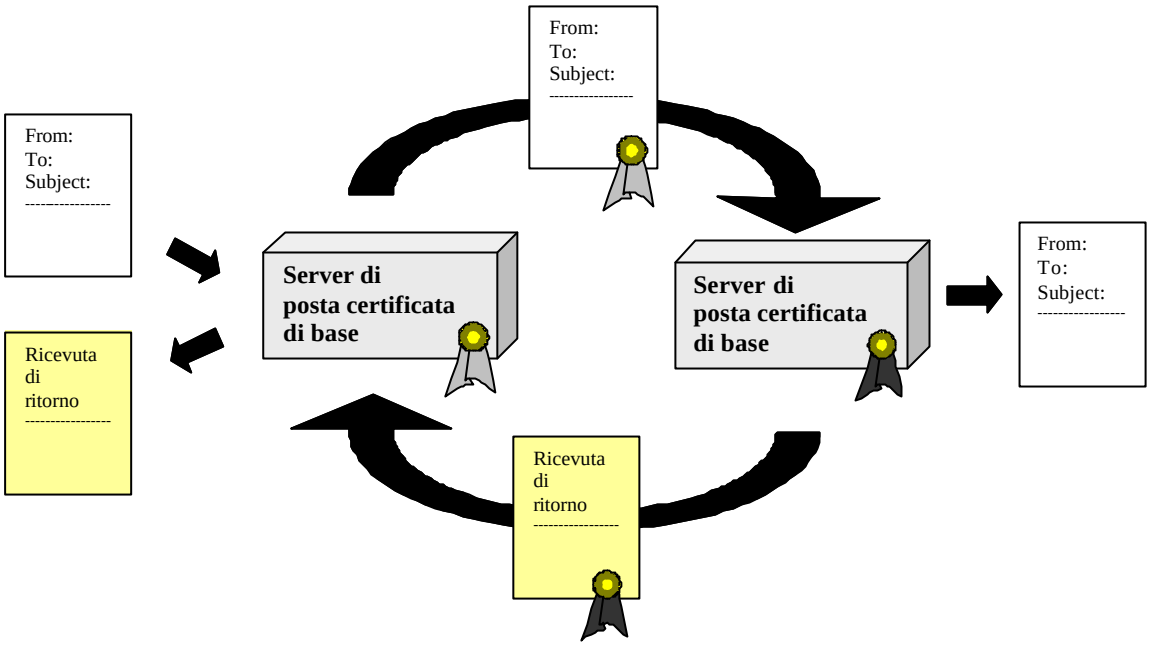
Comprendono i messaggi scambiati tra indirizzi di posta istituzionali non attestati su una AOO; esse sono schematizzate nel diagramma seguente.



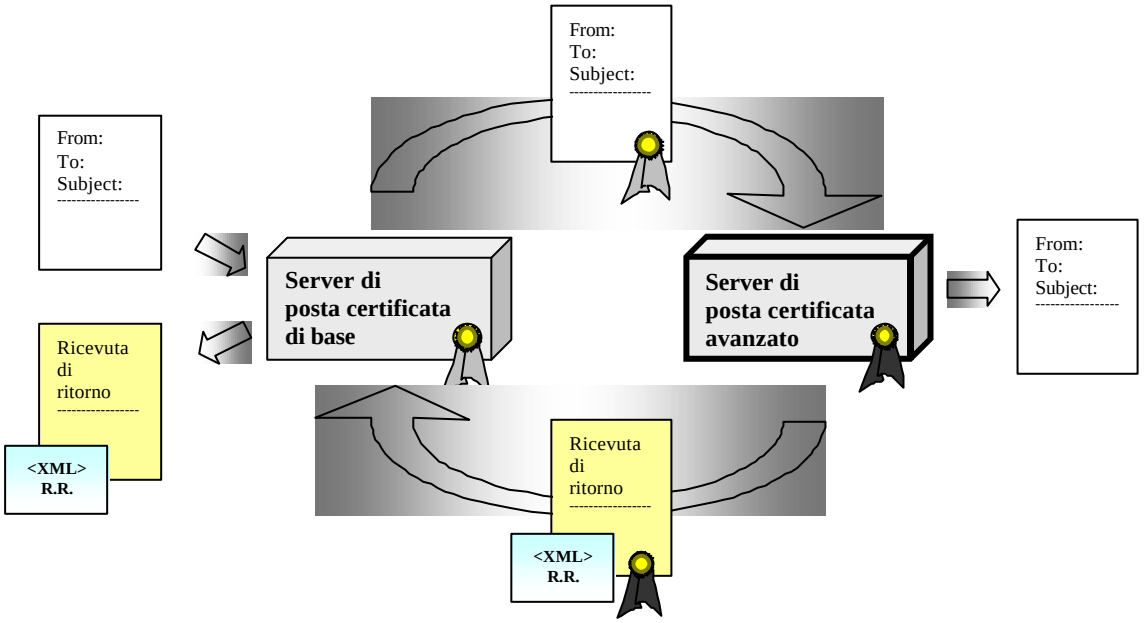
Le fasi principali del processo sono analizzate di seguito:

- creazione messaggio (1:, 2:): il mittente crea il messaggio, eventualmente firmato, e lo sottopone al proprio servizio di posta certificata
- spedizione messaggio (3:, 4:, 5:): il servizio di posta certificata mittente appone il proprio MAC e spedisce il messaggio di posta certificata, dopo aver aggiornato il log di posta
- ricezione messaggio (6:, 7:, 12:, 13:): il servizio di posta certificata destinatario autentica il messaggio ricevuto e lo inoltra al destinatario, dopo aver aggiornato il log di posta
- spedizione ricevuta di ritorno (8:, 9:, 10:, 11:): il servizio di posta certificata destinatario crea la ricevuta di ritorno e la spedisce al server mittente: quest'ultimo autentica la ricevuta di ritorno e la inoltra al mittente del messaggio.

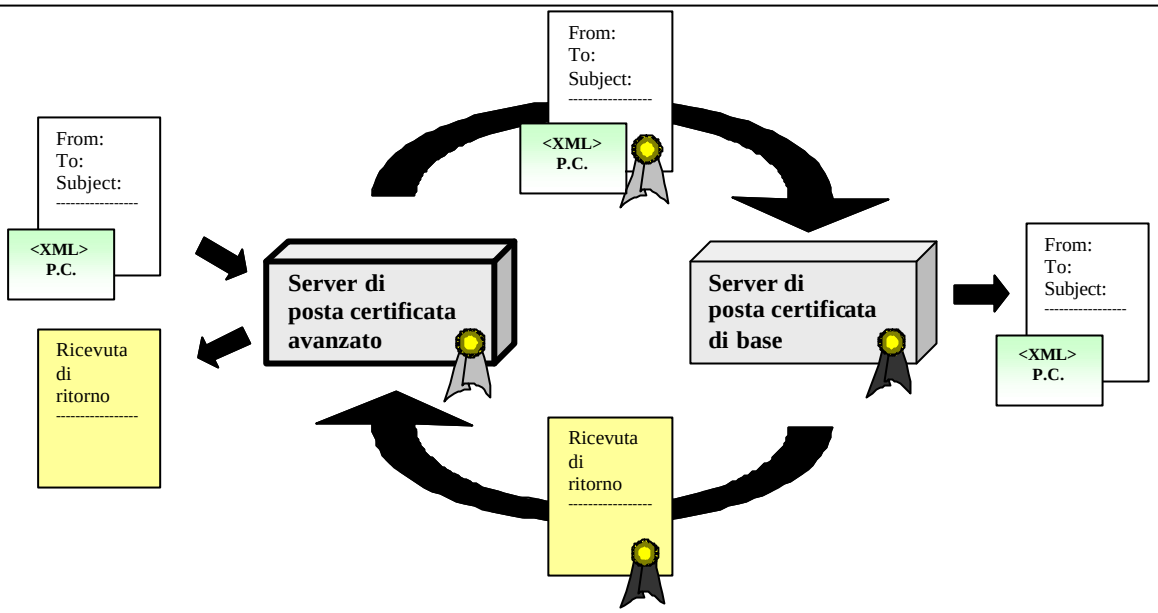
Per analizzare nel dettaglio il formato dei messaggi scambiati bisogna individuare i possibili casi particolari. Essi sono mostrati nei diagrammi seguenti.



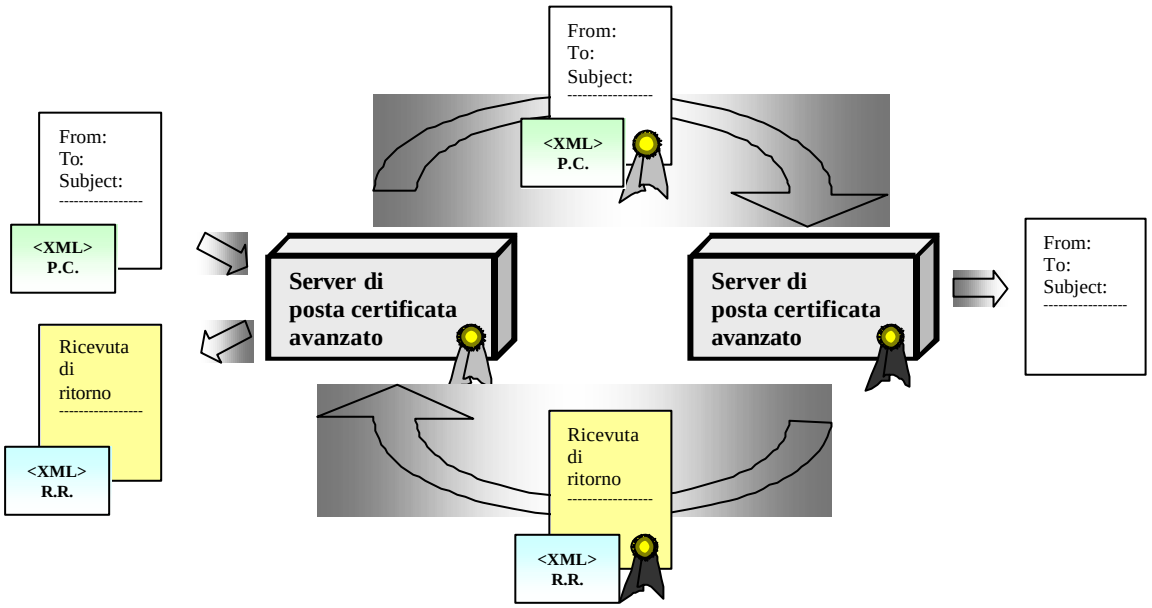
Quando entrambi i server di posta certificata sono di base, come nella figura precedente, i messaggi che vengono scambiati contengono in allegato soltanto i MAC e i certificati dei server.



Se il server di posta certificata destinatario è avanzato (figura precedente), la ricevuta di ritorno contiene in allegato il file "RicevutaRitorno.xml".



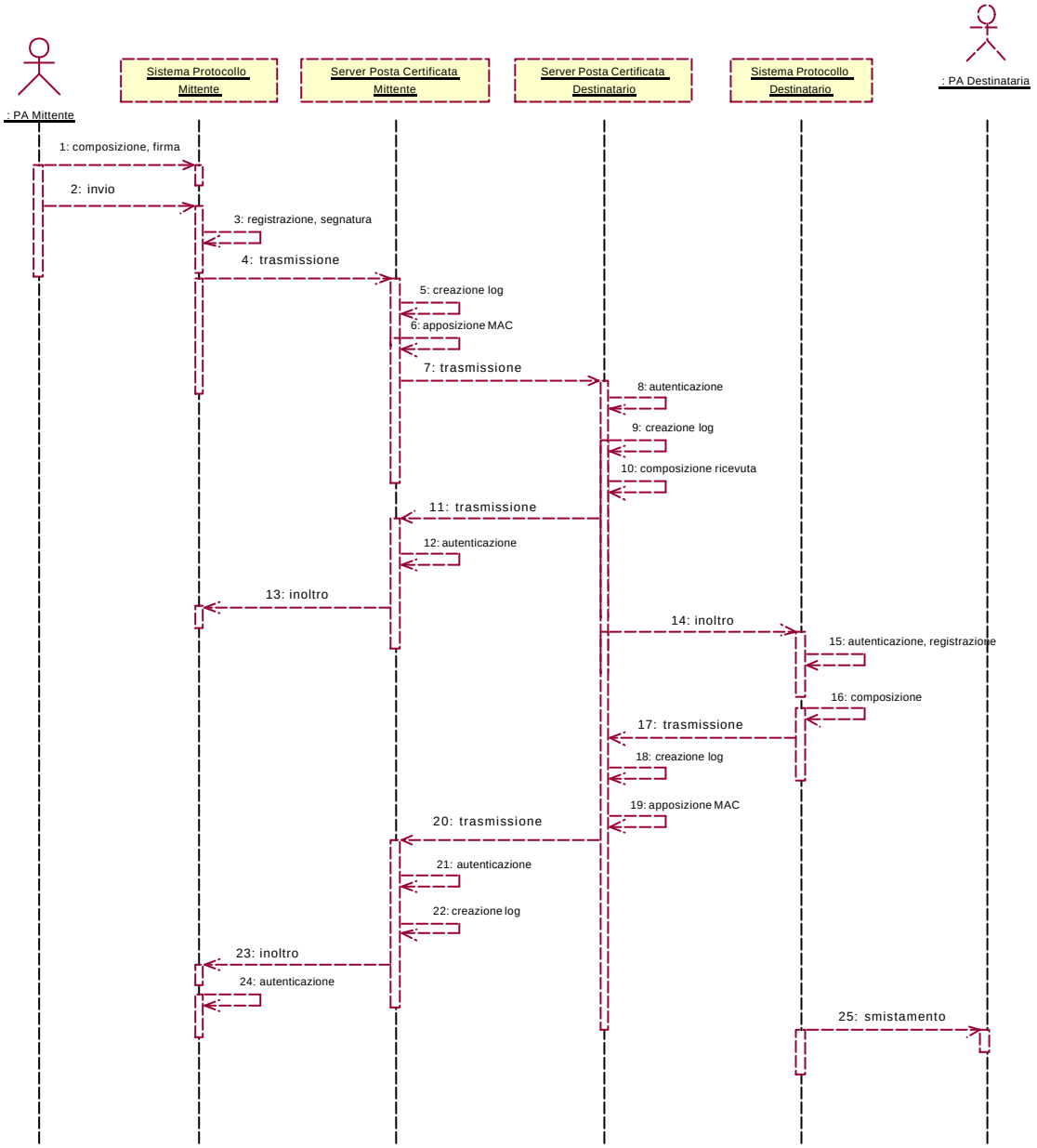
Quando è il server di posta certificata mittente a essere avanzato (figura precedente), il messaggio originario è completato dal file allegato "PostaCertificata.xml": quest'ultimo viene ignorato dal server destinatario e dunque inoltrato al destinatario del messaggio.



Nell'ultimo caso considerato, quando entrambi i server di posta certificata sono avanzati (figura precedente), sia il messaggio originario che la ricevuta di ritorno hanno in allegato i corrispondenti file XML.

Interazioni con i sistemi di protocollo informatico

Lo scenario considerato riguarda i messaggi protocollati scambiati tra indirizzi di posta istituzionali attestati su una AOO; le interazioni esistenti sono schematizzate nel diagramma seguente.

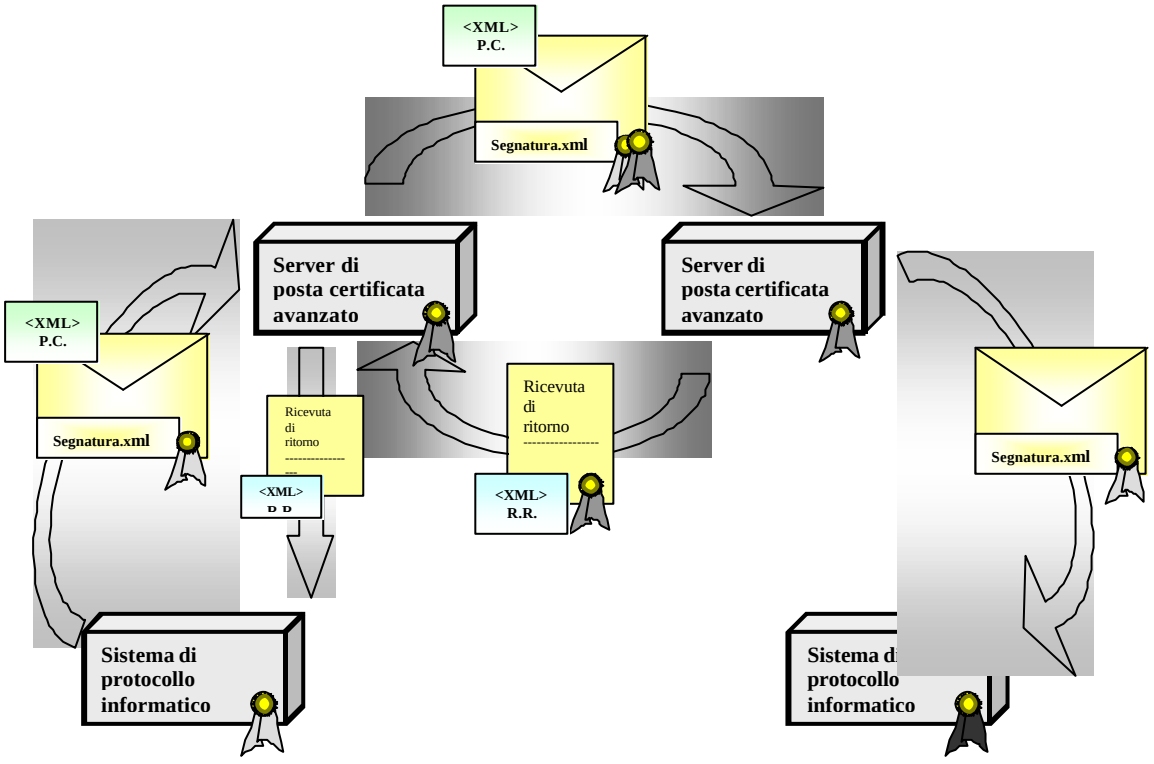


Le fasi principali del processo sono analizzate di seguito:

- creazione messaggio (1:, 2:): il funzionario crea il messaggio, eventualmente firmato, e lo invia al proprio sistema di protocollo
- protocollazione in uscita (3:, 4:): il sistema di Protocollo Informatico mittente appone la segnatura XML e sottopone il messaggio protocollato al proprio servizio di posta certificata: se quest'ultimo è di tipo avanzato, viene aggiunto al messaggio il file "PostaCertificata.xml" contenente le direttive di trattamento del messaggio per il servizio di posta certificata destinatario

- spedizione messaggio (5:, 6:, 7:): il servizio di posta certificata mittente appone il proprio MAC e spedisce il messaggio di posta certificata, dopo aver aggiornato il log di posta
- ricezione messaggio (8:, 9:, 14:): il servizio di posta certificata destinatario autentica il messaggio ricevuto, aggiorna il log di posta, ed inoltra il messaggio al servizio di Protocollo Informatico destinatario
- spedizione ricevuta di ritorno di posta certificata (10:, 11:, 12:, 13:): il servizio di posta certificata destinatario crea la ricevuta di ritorno e la spedisce al mittente, eventualmente in accordo con quanto precisato nel file "PostaCertificata.xml"
- protocollazione in ingresso (15:, 16:, 17:, 25:): il servizio di Protocollo Informatico destinatario elabora il messaggio ricevuto e crea la Conferma di Ricezione sottoponendola al proprio servizio di posta certificata; il messaggio viene smistato verso il funzionario o l'ufficio competente
- spedizione conferma di ricezione (18:, 19:, 20:): il servizio di posta certificata mittente appone il proprio MAC e spedisce il messaggio di posta certificata, dopo aver aggiornato il log di posta
- ricezione conferma di ricezione (21:, 22:, 23:, 24:): il servizio di posta certificata destinatario autentica il messaggio ricevuto e lo inoltra al servizio di Protocollo Informatico mittente, dopo aver aggiornato il log di posta.

Per analizzare nel dettaglio il formato dei messaggi scambiati bisogna individuare i possibili casi particolari. Essi sono mostrati nei diagrammi seguenti, dove vengono considerati soltanto i casi in cui i server di posta certificata siano entrambi avanzati.



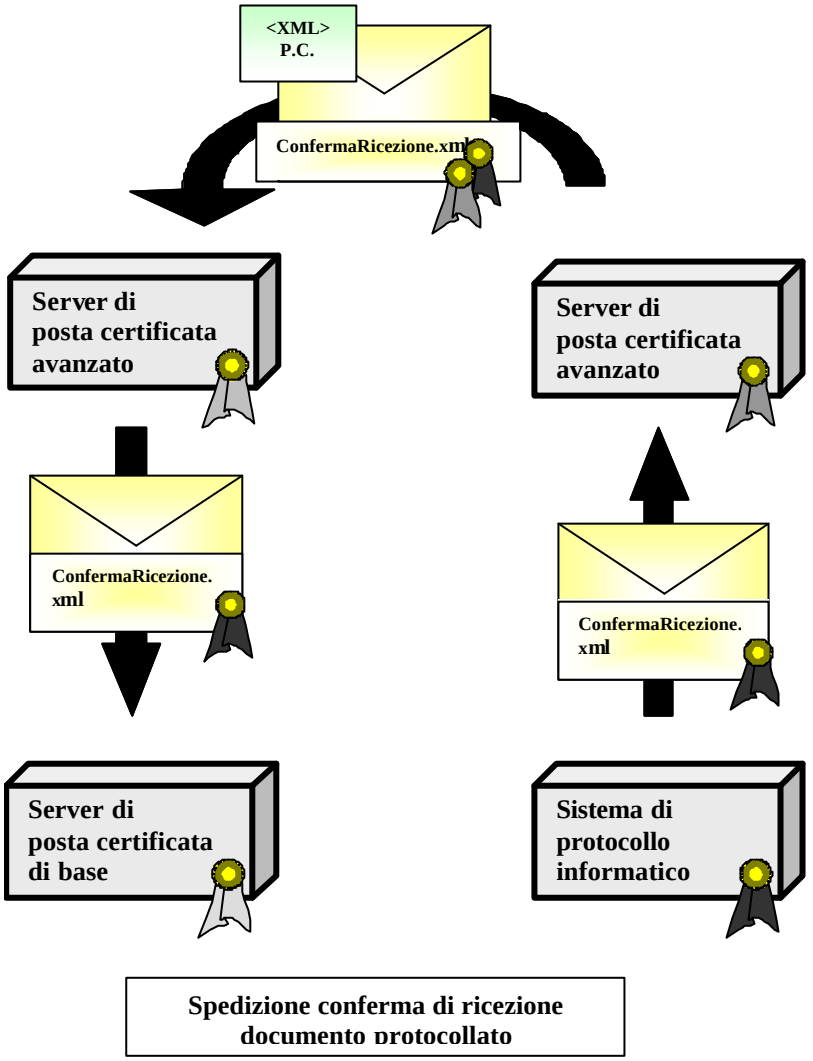
Spedizione documento

In fase di spedizione il sistema di Protocollo Informatico mittente crea un messaggio che contiene il file "Segnatura.xml", le informazioni che lo autenticano e aggiunge in allegato il file "PostaCertificata.xml".

Il server di posta certificata mittente aggiunge il MAC e il proprio certificato.

Il server di posta certificata destinatario toglie il MAC, il certificato e l'allegato XML e inoltra al sistema di protocollo informatico destinatario solo il messaggio e la segnatura. Esso inoltre produce la ricevuta di ritorno e le informazioni di autenticazione.

Infine il server di posta certificata destinatario elimina le informazioni di autenticazione e recapita al sistema di Protocollo Informatico mittente la ricevuta di ritorno corredata dall'allegato "RicevutaRitorno.xml".



Il sistema di protocollo informatico destinatario crea una conferma di ricezione, un messaggio che contiene il file "ConfermaRicezione.xml", le informazioni che lo autenticano e lo sottopone al proprio server di posta certificata.

Questo aggiunge il MAC con il proprio certificato e allega il file "PostaCertificata.xml"; in questo esempio si suppone che nelle istruzioni che questo contiene sia specificata la direttiva di non spedire la ricevuta di ritorno: questa scelta è dovuta alla considerazione che la ricevuta di ritorno sia in questo caso poco significativa, preferendo al contrario uno snellimento del meccanismo.

Infine il server di posta certificata destinatario elimina le informazioni di autenticazione e recapita al sistema di protocollo informatico mittente la ricevuta di ritorno corredata dall'allegato "RicevutaRitorno.xml".