Cittadinanza Digitale

Valutazione d'impatto sulla protezione dei dati

Team per la Trasformazione Digitale
Agenzia per L'Italia Digitale

31 Maggio 2018

Indice

1 Introduzione

1.1 Cittadinanza Digitale

La Presidenza del Consiglio dei Ministri, in collaborazione con l'Agenzia per l'Italia Digitale, ha progettato e sviluppato un sistema applicativo che si presenta come il punto di accesso ai servizi delle pubbliche amministrazione e degli altri soggetti pubblici indicati all'articolo 2, comma 2, del CAD (di seguito, "Enti Erogatori"), quali appunto le società a controllo pubblico, non quotate, e i gestori di pubblici servizi.

Tale sistema applicativo è fruibile attraverso la relativa applicazione mobile, scaricabile gratuitamente dallo store preferito dall'utente cittadino, disponibile per piattaforma sia Android, sia iOS. Le funzionalità legate alla gestione dell'account, della privacy e della sicurezza saranno disponibili anche tramite browser web.

L'applicazione di Cittadinanza Digitale (CD) rappresenta un canale complementare o alternativo agli altri canali digitali già utilizzati dagli Enti Erogatori, attraverso cui gli enti stessi metteranno a disposizione dell'utente le funzioni descritte in seguito e relative ai propri servizi.

CD, infatti, attraverso un'unica piattaforma applicativa consente al cittadino di interagire con le amministrazioni italiane, centrali e locali, e con gli Enti Erogatori per l'erogazione di specifici servizi digitali dagli stessi forniti. CD, pertanto, assume un duplice valore in quanto, da un lato, offre ai soggetti pubblici una serie di funzioni che tradizionalmente sono comuni a tutti i servizi digitali e, dall'altro, offre agli utenti cittadini uno strumento unico per fruire di queste stesse funzioni.

CD nella sua funzione di punto di accesso, permette all'utente di accedere facilmente ed in modalità aggregata alle proprie informazioni ed ai servizi digitali che lo riguardano, indipendentemente da quali siano gli Enti Erogatori di suo specifico interesse. CD non si sostituisce in alcun modo agli Enti Erogatori, che rimangono pertanto titolari delle informazioni in loro possesso, dei relativi trattamenti di dati personali e dell'erogazione dei relativi servizi, che restano nella loro disponibilità esclusiva. Per questo CD si configura semplicemente con un canale supplementare funzionale affinché l'utente possa raggiungere, più facilmente e in modalità più razionalizzata, le informazioni e i servizi degli Enti Erogatori.

Ferma ogni possibile implementazione nel tempo da parte della Presidenza del Consiglio dei Ministri di altre funzionalità, allo stato attuale, l'applicazione di CD si compone di 5 sezioni principali, che corrispondono a cinque funzioni base comuni a molti servizi digitali:

- Messaggi;
- portafoglio;
- documenti;
- preferenze;
- profilo.

L'utente, previo l'opportuno download dell'applicazione in un dispositivo compatibile, potrà accedere ai servizi, autenticandosi tramite SPID. Disporre di un account SPID valido sarà quindi condizione necessaria e sufficiente per utilizzare CD.

Si descrivono di seguito le sezioni principali di cui si compone CD, che corrispondono ad altrettante funzioni disponibili ai soggetti pubblici.

1.1.1 Servizio messaggi

La sezione messaggi consentirà all'utente di ricevere le comunicazioni a lui indirizzate da parte degli Enti Erogatori che utilizzano le api messe a disposizione da CD e dagli altri servizi collegati.

L'utente potrà ordinare e/o filtrare i messaggi ricevuti sulla base di distinti parametri, quali, ad esempio, la data di invio del messaggio, l'identificativo del servizio oggetto del messaggio, l'oggetto indicato nel messaggio, etc. Altri metadati ed altre funzioni di ricerca/ordinamento potranno essere integrate nelle successive versioni di CD.

L'utente, se lo desidera, potrà beneficiare di ulteriori funzionalità collegate, quali la possibilità di gestire le preferenze di recapito per uno specifico servizio, condividere con terzi il messaggio, ricevere degli avvisi in merito alla scadenza del messaggio, etc.

Per gli Enti Erogatori che aderiscono a CD sarà possibile interrogare un servizio per sapere se uno specifico cittadino ha attivato CD e se ha delle preferenze relative all'ente stesso.

1.1.2 Portafoglio

La sezione portafoglio, integrata con il Sistema pagoPA, consente di gestire le transazioni economiche fra il cittadino e lo stato, gestire i propri metodi di pagamento preferiti e di avere a disposizione la lista delle transazioni già eseguite, al pari delle più comuni applicazioni per i servizi di home banking.

Le funzioni di pagamento consentiranno di eseguire le transazione economiche anche all'interno della stessa app di CD.

Se l'utente è censito nel sistema pagoPA potrà trovare nell'app lo storico di alcune delle transazioni effettuate e le relative ricevute anche prima dell'attivazione di CD.

L'utente in CD potrà salvare e gestire i metodi di pagamento previsti dal sistema PagoPA.

1.1.3 Documenti

La sezione documenti consente all'utente di tenere raccolti e da lui organizzati dentro CD tutti i documenti che gli sono stati inviati o messi a disposizione dagli Enti Erogatori.

I documenti saranno filtrabili e ricercabili secondo una serie di parametri descritti dalle specifiche tecniche di CD, quali ad esempio data, tipologia, titolo, descrizione, etc.

Gli Enti Erogatori dovranno mettere a disposizione, oltre al documento, il set di metadati che consentono una corretta indicizzazione e ricerca sul documento, come descritto nelle specifiche tecniche di CD per le quali si rinvia all'allegato tecnico.

I documenti, ad esempio i certificati, che non sono disponibili potranno essere richiesti direttamente dall'utente all'interno di CD, a condizione che il processo di definizione delle caratteristiche del documento stesso consentano una esperienza d'uso semplice e adatta ad un dispositivo mobile.

Gli Enti Erogatori dovranno semplificare il più possibile il processo di generazione del documento o del certificato, così da renderlo compatibile con la richiesta e la distribuzione tramite CD, e dovranno censire nel sistema CD i documenti che sono in grado di erogare attraverso il sistema stesso.

Eventuali costi associati alla generazione di alcuni di questi documenti e certificati (come, ad esempio, marche da bollo e/o diritti di segreteria) potranno essere sostenuti direttamente attraverso le funzioni di pagamento disponibili nella sezione portafoglio di CD.

Tutti i documenti erogati dagli Enti Erogatori devono essere in formato digitale, devono avere il set di metadati descritto nelle specifiche tecniche di CD, e devono essere resi disponibili, altresì, in modo da garantire per l'utente l'esperienza qui sopra descritta.

A titolo di esempio, si segnala l'integrazione con ANPR (Anagrafe Nazionale della Popolazione Residente), che consentirà di inoltrare la richiesta di un certificato anagrafico ai comuni già integrati con ANPR, ottenendo da essi il certificato richiesto direttamente con l'applicazione di CD.

1.1.4 Preferenze

La sezione preferenze consente all'utente di impostare quelle scelte di carattere generale che risultano trasversali all'erogazione dei servizi da parte della pubblica amministrazione. Alcune di queste scelte, una volta inserite dall'utente potranno essere interrogate e utilizzate in tempo reale dagli Enti Erogatori che aderiscono a CD.

Di seguito, si riportano a titolo di esempio alcune preferenze che potranno essere definite dell'utente:

- Lingua, da scegliere tra italiano, inglese o tedesco (interrogabile);
- email personale dell'utente;
- elenco dei servizi che l'utente può attivare e relativa modalità di recapito da scegliere tra messaggio sull'applicazione mobile, notifica push sul cellulare, messaggio email;
- elezione, modifica o disattivazione del domicilio digitale dell'utente (interrogabile).

A ciascun Ente Erogatore sarà chiesto di fornire un insieme base di informazioni che comporranno una scheda ente, ed un equivalente insieme di informazioni base per ciascuno dei servizi che usano le funzioni di CD. Queste informazioni potranno essere esposte in CD all'interno di una sezione dedicata a ciascun ente/servizio, collegata alle preferenze di quel servizio stesso.

Con riferimento alla selezione delle preferenze, appare opportuno segnalare che:

- La selezione da parte dell'utente del servizio di inbox, determina l'invio da parte degli Enti Erogatori di un messaggio di notifica al cittadino che genera la presenza del messaggio nella schermata Messaggi dell'applicazione mobile di CD sullo smartphone dell'utente;
- la selezione da parte dell'utente del servizio di ricezione via email, determina l'invio da parte degli Enti Erogatori di un messaggio di notifica al cittadino che genera una email ricevuta nella casella di posta indicata dall'utente;
- la selezione da parte dell'utente del servizio di notifica push, determina l'invio da parte degli Enti Erogatori di un messaggio di notifica push sullo smartphone indicato dall'utente.

1.1.5 Profilo

La sezione Pprofilo, che sarà disponibile anche tramite browser web, consente all'utente di avere un riepilogo delle informazioni più tipicamente legate alla propria identità.

In questa sezione, infatti, l'utente potrà accedere e verificare i dati anagrafici acquisiti da CD tramite il login effettuato con SPID.

L'eventuale aggiornamento di dati anagrafici in CD non verrà propagato agli Identity Provider SPID.

Nella stessa sezione Profilo l'utente potrà gestire eventuali strumenti complementari di identificazione e sicurezza quali PIN o, se abilitati dall'utente sul proprio dispositivo, strumenti di identificazione biometrica, e potrà interrompere la sessione attualmente attiva sull'applicazione (logout).

Nella sezione profilo l'utente potrà vedere le proprie informazioni anagrafiche, messe a disposizione dell'utente tramite un'integrazione con ANPR, a condizione che il Comune di residenza dell'utente sia già subentrato in ANPR.

Nella sezione profilo l'utente potrà inoltre verificare i termini e condizioni d'uso del servizio in vigore, consultare le informative sul trattamento dei dati personali degli Enti Erogatori e una breve informativa relativa a CD, chiedere la sospensione dell'account o la completa cancellazione dello stesso.

1.2 Motivazioni alla base della valutazione d'impatto

1.2.1 Gestione di dati personali

Tramite le funzionalità dei Messaggi e Documenti, la piattaforma informatica di CD tratterà documenti personali e messaggi di cortesia equiparabili a messaggi di posta elettronica. Inoltre, per quanto riguarda la funzionalità di Profilo, la piattaforma informatica di CD tratterà metadati relativi ai servizi ed Enti Erogatori da cui un cittadino a ricevuto messaggi di cortesia e avvisi di pagamento.

1.2.2 Trattamento di dati su larga scala

L'obiettivo di CD è quello di fornire un servizio a tutta la popolazione italiana dotata di account SPID. Si concretizza quindi lo scenario del trattamento di dati su larga scala.[1]

2 Descrizione dei flussi informativi

TODO The collection, use and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining

[1] Cfr. *Linee guida sui responsabili della protezione dei dati (RPD)* del WP29 - 16/EN WP 243.

data flows. You should also say how many individuals are likely to be affected by the project.

Explain how information will be obtained, used, and retained – there may be several options to consider. This step can be based on, or form part of, a wider project plan.

1. This process can help to identify potential 'function creep' - unforeseen or unintended uses of the data (for example data sharing)
2. People who will be using the information are consulted on the practical implications.
3. Potential future uses of information are identified, even if they are not immediately necessary.

2.1 Funzionalità Messaggi

La funzionalità Messaggi di CD implementa delle logiche di gestione del dato che variano a seconda della tipologia di messaggio e della configurazione delle preferenze del cittadino a cui è indirizzato lo stesso.

Possiamo innanzitutto classificare i possibili scenari in due macro gruppi:

1. La gestione del messaggio quando il cittadino destinatario NON ha ancora effettuato il primo accesso all'applicazione di CD;
2. La gestione del messaggio quando il cittadino destinatario ha già effettuato il primo accesso all'applicazione di CD;

Questa distinzione è importante poichè quando il cittadino non ha ancora effettuato il primo accesso all'applicazione di CD, la funzionalità di invio messaggi di CD è equiparabile ad un servizio di email transazionale.[2]

2.1.1 Invio di messaggi a destinatari non ancora censiti

```
Alice -> Bob: Authentication Request
Bob --> Alice: Authentication Response

Alice -> Bob: Another authentication Request
Alice <-- Bob: another authentication Response
```

[2] si veda per esempio il servizio MailUP usato da molte Pubbliche Amministrazioni per l'invio di avvisi di cortesia via email ai cittadini.

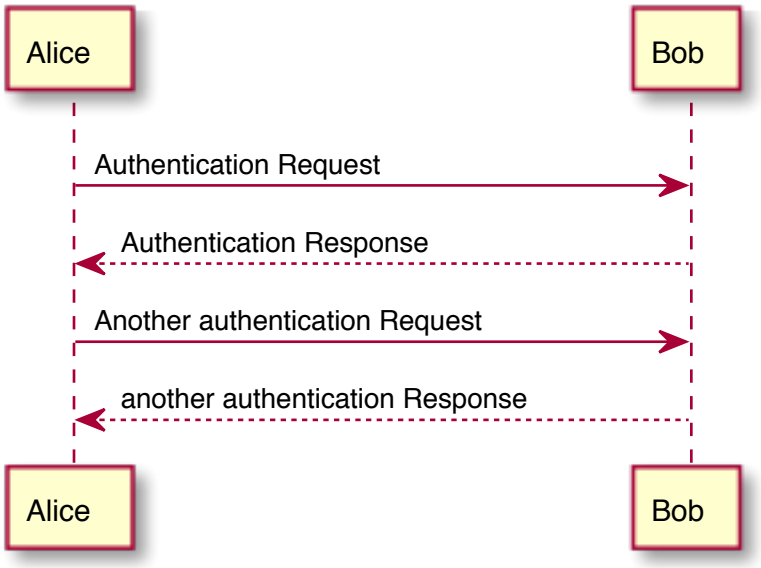

Figura 1: diagram1

2.1.2 Invio di messaggi a destinatari censiti

3 Processo di analisi

TODO Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process. Consultation can be used at any stage of the PIA process.

4 Analisi dei rischi

TODO Identify the key privacy risks and the associated compliance and corporate risks.

Record the risks to individuals, including possible intrusions on privacy where appropriate.

1. Assess the corporate risks, including regulatory action, reputational damage, and loss of public trust.

2. Conduct a compliance check against the Data Protection Act and other relevant legislation.
3. Maintain a record of the identified risks.
4. The process helps an organisation to understand the likelihood and severity of privacy risks.
5. An organisation is open with itself about risks and potential changes to a project.

4.1 (Oggetto)

4.1.1 Rischi per le persone

TODO

4.1.2 Rischi di aderenza

TODO

4.1.3 Rischi per l'organizzazione

TODO

5 Soluzioni adottate

TODO Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Devise ways to reduce or eliminate privacy risks.

1. Assess the costs and benefits of each approach, looking at the impact on privacy and the effect on the project outcomes.
2. Refer back to the privacy risk register until satisfied with the overall privacy impact.
3. The process takes into account the aims of the project and the impact on privacy.

4. The process also records privacy risks which have been accepted as necessary for the project to continue.

5.1 (Rischio)

5.1.1 Soluzione

5.1.2 Risultato

is the risk eliminated, reduced, or accepted?

5.1.3 Valutazione

is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

6 Stato di approvazione

TODO Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Obtain appropriate signoff within the organisation.

1. Produce a PIA report, drawing on material produced earlier during the PIA.
2. Consider publishing the report or other relevant information about the process.
3. The PIA is approved at a level appropriate to the project.
4. A PIA report or summary is made available to the appropriate stakeholders.

Rischio	Soluzione	Approvata da

7 Stato di implementazione

TODO Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?

Ensure that the steps recommended by the PIA are implemented.

1. Continue to use the PIA throughout the project lifecycle when appropriate.
2. The implementation of privacy solutions is carried out and recorded.
3. The PIA is referred to if the project is reviewed or expanded in the future.

Risultato da conseguire	Data prevista	Responsabile