eGovernment

CONTESTO

- Piano eGov, Avvisi eGov
- Agenda Digitale UE
- Agenda Digitale Italiana
- Piano Telematico E-R

R-INNOVAZIONE

- Tecnologia
- Normativa e prassi
  - legittimità ed efficacia
- Organizzazione
  - riprogettazione dei processi
  - formazione (dal digital divide al valore aggiunto)

INFORMATICA GIURIDICA

- metodo interdisciplinare che coniuga diverse competenze
  - ridisegnare i modelli organizzativi alla luce dei nuovi strumenti tecnologici
    - modello interdisciplinare volto a creare realtà di semplificazione, interoperabilità, contenimento della spesa ed efficienza
  - supportare con un robusto impianto normativo
    - potenziare l'azione effettiva del diritto nei processi di innovazione

LIBRI e CONVERSAZIONI

Biblioteca dell'Assemblea Legislativa della Regione Emilia-Romagna

E-Government

Bologna, 18 novembre 2013

eGovernment

CONTESTO

- Piano eGov, Avvisi eGov
- Agenda Digitale UE
- Agenda Digitale Italiana
- Piano Telematico E-R

R-INNOVAZIONE

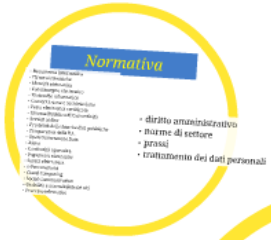
- Tecnologia
- Normativa e prassi
  - legittimità ed efficacia
- Organizzazione
  - riprogettazione dei processi
  - formazione (dal digital divide al valore aggiunto)

INFORMATICA GIURIDICA

- metodo interdisciplinare che coniuga diverse competenze
  - ridisegnare i modelli organizzativi alla luce dei nuovi strumenti tecnologici
    - modello interdisciplinare volto a creare realtà di semplificazione, interoperabilità, contenimento della spesa ed efficienza
  - supportare con un robusto impianto normativo
    - potenziare l'azione effettiva del diritto nei processi di innovazione

CONTESTO

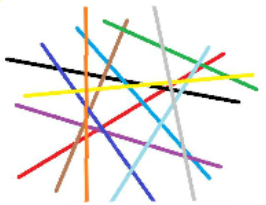
- Piano eGov, Avvisi eGov
- Agenda Digitale UE
- Agenda Digitale Italiana
- Piano Telematico E-R



Machiavelli

«E debbesi considerare come non è cosa più difficile a trattare, nè più dubbia a riuscire, nè più pericolosa a maneggiare, che farsi capo ad introdurre nuovi ordini. Perchè l'introduttore ha per nimici tutti coloro che degli ordini vecchi fanno bene; e tepidi difensori tutti quelli che degli ordini nuovi farebbono bene; la qual tepidezza nasce, parte per paura degli avversari, che hanno le leggi in beneficio loro, parte dalla incredulità degli uomini, i quali non credono in verità le cose nuove, se non ne veggono nata esperienza ferma»

Il Principe, 1513



INVARIANZA

Dall'attuazione del presente decreto non devono derivare nuovi o maggiori oneri a carico della finanza pubblica

Normativa

- Documento informatico
- Firme elettroniche
- Identità elettronica
- Contrassegno elettronico
- Protocollo informatico
- Conservazione e archiviazione
- Posta elettronica certificata
- Sistema Pubblico di Connettività
- Servizi online
- Fruibilità delle banche dati pubbliche
- Trasparenza della P.A.
- Open Government Data
- Riuso
- Continuità operativa
- Pagamenti elettronici
- Sanità elettronica
- e-Procurement
- Cloud Computing
- Social Communication
- Usabilità e accessibilità dei siti
- Processo telematico

- diritto amministrativo
- norme di settore
- prassi
- trattamento dei dati personali

Machiavelli

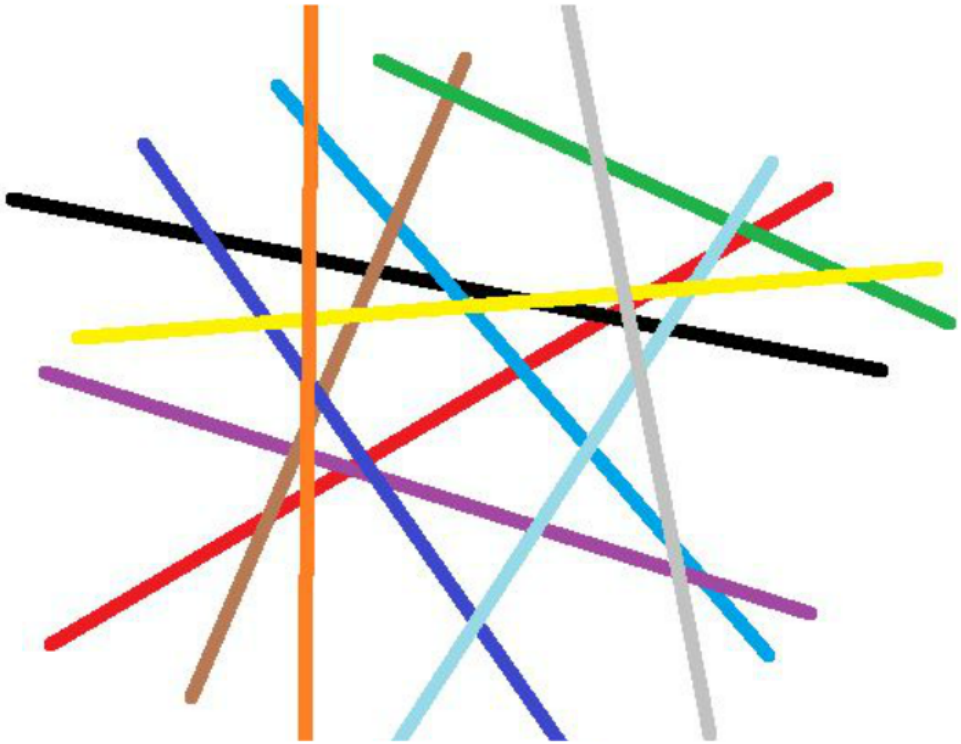
«E debbesi considerare come non è cosa più difficile a trattare, nè più dubbia a riuscire, nè più pericolosa a maneggiare, che farsi capo ad introdurre nuovi ordini.
Perchè l'introduttore ha per nimici tutti coloro che degli ordini vecchi fanno bene; e tepidi difensori tutti quelli che degli ordini nuovi farebbono bene; la qual tepidezza nasce, parte per paura degli avversari, che hanno le leggi in beneficio loro, parte dalla incredulità degli uomini, i quali non credono in verità le cose nuove, se non ne veggono nata esperienza ferma»

Il Principe, 1513

INVARIANZA

Dall'attuazione del presente decreto non devono derivare nuovi o maggiori oneri a carico della finanza pubblica

Dall'a
decre
nuov
della



SHANGHAI

eGovernment

CONTESTO

- Piano eGov, Avvisi eGov
- Agenda Digitale UE
- Agenda Digitale Italiana
- Piano Telematico E-R

R-INNOVAZIONE

- Tecnologia
- Normativa e prassi
  - legittimità ed efficacia
- Organizzazione
  - riprogettazione dei processi
  - formazione (dal digital divide al valore aggiunto)

INFORMATICA GIURIDICA

- metodo interdisciplinare che coniuga diverse competenze
  - ridisegnare i modelli organizzativi alla luce dei nuovi strumenti tecnologici
    - modello interdisciplinare volto a creare realtà di semplificazione, interoperabilità, contenimento della spesa ed efficienza
  - supportare con un robusto impianto normativo
    - potenziare l'azione effettiva del diritto nei processi di innovazione

R-INNOVAZIONE

- Tecnologia
- Normativa e prassi
    - legittimità ed efficacia
- Organizzazione
    - riprogettazione dei processi
    - formazione (dal digital divide al valore aggiunto)

Se vuoi viaggiare veloce
viaggia da solo
ma se vuoi andare lontano
viaggia in compagnia
(proverbio africano)

Se vuoi viaggiare veloce
viaggia da solo
ma se vuoi andare lontano
viaggia in compagnia
(proverbio africano)

INFORMATICA GIURIDICA

- metodo interdisciplinare che coniuga diverse competenze
  - ridisegnare i modelli organizzativi alla luce dei nuovi strumenti tecnologici
    - modello interdisciplinare volto a creare realtà di semplificazione, interoperabilità, contenimento della spesa ed efficienza
  - supportare con un robusto impianto normativo
    - potenziare l'azione effettiva del diritto nei processi di innovazione

(alcuni) Progetti

Decertificazione

- modelli informatico-giuridici per la validazione di strumenti di emissione di dichiarazioni sostitutive online
- possibilità di controllo da parte della PA ricevente

Firme elettroniche remote

- procedimento di sottoscrizione della firma digitale
- modalità operative
- dispositivo TSM

Fruibilità delle banche dati pubbliche

- condivisione dei dati fra pubbliche amministrazioni
- convenzioni fra enti
- misure di sicurezza
- misure volte a salvaguardare la proporzionalità, liceità e necessità del trattamento

D.I.A. telematica del Comune di Ravenna

- peculiarità del tipo di atto
- modalità di telematizzazione ed informatizzazione del procedimento
- accesso al servizio da parte del cittadino
- intermediazione e delega

Sanità elettronica

- identità elettronica
- trattamento dei dati sanitari
- impiego di piattaforme di cloud computing in sanità
- situazioni di emergenza e accesso ai dati

Identità federata

- modalità di identificazione del cittadino che accede ai servizi
- modalità di sottoscrizione delle istanze inviate al cittadino
- accordi fra gli enti federati
- misure volte a salvaguardare il livello complessivo del servizio

Privacy e pubblicità istituzionale - trasparenza -

- dovere di pubblicazione, pubblicità delle attività istituzionali
- limiti conseguenti alla protezione dei dati personali
- durata della pubblicazione
- diritto all'oblio

Cloud Computing

- analisi contrattuale
- tutela dei dati personali
- continuità operativa
- rilevanza e peculiarità della funzione pubblica, analisi dei costi ed effettivo beneficio della PA

Open Government Data

- percorso di apertura dei dati pubblici
- scelta dei dati
- formato dei dati
- metadati
- licenze e interoperabilità delle licenze
- laboratori con i settori
- questionario

DEC

- Univer
- serv
- i

Decertificazione

- modelli informatico-giuridici per la validazione di strumenti di emissione di dichiarazioni sostitutive online
- possibilità di controllo da parte della PA ricevente

Firme elettroniche remote

- procedimento di apposizione della firma digitale
- modalità remotizzata
- dispositivo HSM

Fruibilità delle banche dati pubbliche

- condivisione dei dati fra pubbliche amministrazioni
- convenzioni fra enti
- misure di sicurezza
- misure volte a salvaguardare la proporzionalità, liceità e necessità del trattamento

D.I.A. telematica del Comune di Ravenna

- peculiarità del tipo di atto
- modalità di telematizzazione ed informatizzazione del procedimento
- accesso al servizio da parte del cittadino
- intermediazione e delega

Sanità elettronica

- identità elettronica
- trattamento dei dati sanitari
- impiego di piattaforme di cloud computing in sanità
- situazioni di emergenza e accesso ai dati

Identità federata

- modalità di identificazione del cittadino che accede ai servizi
- modalità di sottoscrizione delle istanze inviate al cittadino
- accordi fra gli enti federati
- misure volte a salvaguardare il livello complessivo del servizio

Privacy e pubblicità istituzionale - trasparenza -

- dovere di pubblicazione, pubblicità delle attività istituzionali
- limiti conseguenti alla protezione dei dati personali
- durata della pubblicazione
- diritto all'oblio

Cloud Computing

- analisi contrattuale
- tutela dei dati personali
- continuità operativa
- rilevanza e peculiarità della funzione pubblica, analisi dei costi ed effettivo beneficio della PA

Open Government Data

- percorso di apertura dei dati pubblici
- scelta dei dati
- formato dei dati
- metadati
- licenze e interoperabilità delle licenze
- laboratori con i settori
- questionario

DECERTIFICAZIONE

- Università di Modena e Reggio-Emilia
  - servizio di certificazione online
    - illegittimità del servizio
      - conversione del servizio

COMUNE DI RAVENNA

SERVIZI DEMOGRAFICI

IL BOLLO DEVE ESSERE APPLICATO ED ANNULLATO NELLA STESSA GIORNATA DI RILASCIO DEL CERTIFICATO

RISULTANZA DI NASCITA

IL SINDACO

In conformita' alle risultanze degli atti d'ufficio

CERTIFICA CHE:

risulta nato il
Atto n. p.1 s.A u. 1

Motivo richiesta: t1

Ravenna , 06-07-2010

IL SINDACO

Firma autografa sostituita ex art. 15 quinquies della Decreto-Legge 28/12/1989 n. 415 convertito con modifiche dall'art. 1 della Legge 28/2/1990 n. 38

Certificato emesso in conformità alle disposizioni del Ministero dell'Interno del 18/2/2009 PGN 0014674 depositate agli atti del Comune di Ravenna

Codici bidimensionali:
http://www.secure-edge.com/files/TIREL_raffronto_codici2D_[1.2].pdf

Linee guida AGID:
http://www.digitpa.gov.it/sites/default/files/notizie/Circolare%20n.%2062%20recante%20Linee%20guida%20contrassegno%20elettronico%20art.%2023%20ter%20CAD_0.pdf

Firma automatica
(art. 1, dpcm 22.2.2013)

- r) **firma automatica**: particolare procedura informatica di firma elettronica qualificata o di firma digitale eseguita previa autorizzazione del sottoscrittore che mantiene il controllo esclusivo delle proprie chiavi di firma, **in assenza di presidio puntuale e continuo da parte di questo**;

Firma automatica
(art. 35, 2-3, CAD)

1. I dispositivi sicuri e le procedure utilizzate per la generazione delle firme devono presentare requisiti di sicurezza tali da garantire che la **chiave privata**: a) sia **riservata**; b) non possa essere derivata e che la relativa firma sia protetta da **contraffazioni**; c) possa essere sufficientemente protetta dal titolare dall'uso da parte di **terzi**.
2. I dispositivi sicuri e le procedure di cui al comma 1 devono garantire l'integrità dei documenti informatici a cui la firma si riferisce. **I documenti informatici devono essere presentati al titolare, prima dell'apposizione della firma, chiaramente e senza ambiguità, e si deve richiedere conferma della volontà di generare la firma** secondo quanto previsto dalle regole tecniche di cui all'articolo 71.
3. Il secondo periodo del comma 2 **non si applica** alle firme apposte con **procedura automatica**. La firma con procedura automatica è valida se apposta **previo consenso del titolare all'adozione della procedura medesima**.

segue

- **(art. 5, c.2)** Il soggetto che appone la sua firma per mezzo di una procedura automatica deve utilizzare **una coppia di chiavi destinata a tale scopo**, diversa da tutte le altre in suo possesso.
- **(art. 5, c.2)** L'utilizzo di tale procedura deve essere indicato esplicitamente nel **certificato qualificato**.

Firma remota
(art. 1, dpcm 22.2.2013)

- q) **firma remota**: particolare procedura di firma elettronica **qualificata** o di firma digitale, generata su HSM, che consente di garantire il controllo esclusivo delle **chiavi private** da parte dei titolari delle stesse;

HSM *Hardware Security Module*
(art. 1, dpcm 22.2.2013)

- p) **HSM**: insieme di hardware e software che realizza **dispositivi sicuri** per la generazione delle firme in grado di gestire in modo sicuro una o più coppie di **chiavi crittografiche**;

Firma remota
(art. 3, dpcm 22.2.2013)

- 4. La firma remota di cui all'art. 1, comma 1, lettera q) , è generata su un HSM custodito e gestito, sotto la responsabilità, dal **certificatore accreditato** ovvero **dall'organizzazione di appartenenza dei titolari dei certificati** che ha richiesto i certificati medesimi ovvero **dall'organizzazione che richiede al certificatore di fornire certificati qualificati ad altri soggetti** al fine di dematerializzare lo scambio documentale con gli stessi. Il certificatore deve essere in grado, dato un certificato qualificato, di individuare agevolmente il dispositivo afferente la corrispondente chiave privata.

segue

- 5. Nel caso in cui il dispositivo di cui al comma 4 **non sia custodito dal certificatore**, **egli deve**:
- a) indicare al soggetto che custodisce il dispositivo le procedure operative, gestionali e le misure di sicurezza fisica e logica che tale soggetto è obbligato ad applicare;
- b) effettuare verifiche periodiche sulla corretta applicazione delle indicazioni di cui alla lettera a), che il soggetto che custodisce il dispositivo ha l'obbligo di consentire ed agevolare;
- c) redigere i verbali dell'attività di verifica di cui alla lettera b) che potranno essere richiesti in copia dall'Agenzia ai fini dell'attività di cui all'art. 31 del Codice;
- d) comunicare all'Agenzia il luogo in cui i medesimi dispositivi sono custoditi;

segue

- e) effettuare ulteriori verifiche su richiesta dell'Agenzia consentendo di partecipare anche ad incaricati dello stesso ente;
- f) assicurare che il soggetto che custodisce il dispositivo si impegni a consentire le verifiche di cui alle lettere b) ed e).
- 6. Nel caso in cui il certificatore venga a conoscenza dell'inosservanza di quanto previsto al comma 5, procede alla revoca dei certificati afferenti le chiavi private custodite sui dispositivi oggetto dell'inadempienza.
- 7. La firma remota di cui all'art. 1, comma 1, lettera q) , è realizzata con misure tecniche ed organizzative, esplicitamente approvate, per le rispettive competenze, dall'Agenzia, nell'ambito delle attività di cui agli articoli 29 e 31 del Codice, e da OCSI, per quanto concerne la sicurezza del dispositivo ai sensi dell'art. 35 del Codice, tali da garantire al titolare il controllo esclusivo della chiave privata.

Contrassegno
(art. 23 *ter*, 5, CAD)

- 5. Sulle copie analogiche di documenti amministrativi informatici può essere apposto a stampa un contrassegno, sulla base dei criteri definiti con linee guida dell'Agenzia per l'Italia digitale, tramite il quale è possibile ottenere il documento informatico, ovvero verificare la corrispondenza allo stesso della copia analogica. Il contrassegno apposto ai sensi del primo periodo sostituisce a tutti gli effetti di legge la sottoscrizione autografa e non può essere richiesta la produzione di altra copia analogica con sottoscrizione autografa del medesimo documento informatico. I programmi software eventualmente necessari alla verifica sono di libera e gratuita disponibilità.

Certificati online

DB ENTE

T3 Documento Inf.

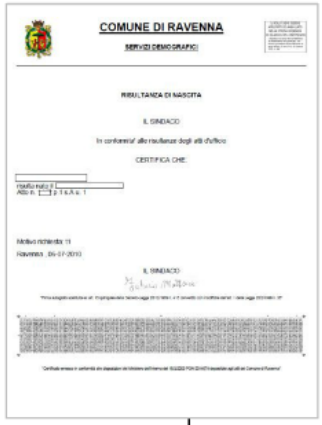
Controlled Workflow

T4 Firma digitale

T5 Contrassegno

HSM

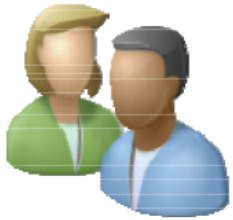
T6 Composizione e presentazione



T2 ISTANZA

T0 PIN chiave privata

T1 Autenticazione



T7 Invio

Premessa in diritto

Certificazioni

- L'art. 15, legge 183/2011 (*rectius* art. 40, d.p.r. 445/2000), dispone:
- «*01. Le certificazioni rilasciate dalla pubblica amministrazione in ordine a stati, qualità personali e fatti* ***sono valide e utilizzabili solo nei rapporti tra privati****. Nei rapporti con gli organi della pubblica amministrazione e i gestori di pubblici servizi* ***i certificati e gli atti di notorietà sono sempre sostituiti dalle dichiarazioni di cui agli articoli 46 e 47***».

segue

- Il successivo comma 02 dispone poi che: «*Sulle certificazioni da produrre ai soggetti privati è apposta, a pena di nullità, la dicitura: "**Il presente certificato <u>non può essere prodotto</u> agli organi della pubblica amministrazione o ai privati gestori di pubblici servizi**"*».

segue

- Al fine della corretta interpretazione dell'articolo dianzi menzionato occorre poi riportare il testo novellato dell'art. 43, d.p.r. 445/2000:
- «*1. Le amministrazioni pubbliche e i gestori di pubblici servizi sono tenuti ad* ***acquisire d'ufficio*** *le informazioni oggetto delle dichiarazioni sostitutive di cui agli articoli 46 e 47, nonché tutti i dati e i documenti che siano in possesso delle pubbliche amministrazioni,* ***previa indicazione, da parte dell'interessato, degli elementi indispensabili per il reperimento delle informazioni o dei dati richiesti****, ovvero* ***ad accettare la dichiarazione sostitutiva prodotta dall'interessato***».

Scenari

- L’attuazione di queste disposizioni conduce, dunque, a due possibili scenari:
- 1) le pubbliche amministrazioni possono realizzare un’infrastruttura d’interoperabilità certificata per lo scambio dei dati su richiesta dell’interessato, con un meccanismo di profilazione e autenticazione dei soggetti coinvolti;
- 2) il soggetto interessato può attestare i propri dati mediante una dichiarazione sostitutiva di certificazione.

- Nell’ambito di attuazione dello **scenario *sub* 1)** si colloca l’art. 58, comma 2, del CAD, il quale dispone che:
- «*2. Ai sensi dell' articolo 50, comma 2, nonché al fine di agevolare **l'acquisizione** d'ufficio ed il **controllo** sulle dichiarazioni sostitutive riguardanti informazioni e dati relativi a stati, qualità personali e fatti di cui agli articoli 46 e 47 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, le **Amministrazioni titolari di banche dati** accessibili per via telematica predispongono, sulla base delle linee guida redatte da DigitPA, sentito il Garante per la protezione dei dati personali, **apposite convenzioni** aperte all'adesione di tutte le amministrazioni interessate volte a disciplinare le modalità di accesso ai dati da parte delle stesse amministrazioni procedenti, senza oneri a loro carico. Le convenzioni valgono anche quale autorizzazione ai sensi dell'articolo 43, comma 2, del citato decreto del Presidente della Repubblica n. 445 del 2000*».

- In merito allo scenario ***sub* 2)** si inserisce, altresì, l'obbligo della pubblica amministrazione ricevente di **accertare**, anche **a campione**, **la veridicità** della **dichiarazione sostitutiva** prodotta dall'interessato.

Idonei controlli

- In argomento l'art. 71 del d.p.r. 445/2000 dispone:
- «*1. Le amministrazioni procedenti sono tenute ad effettuare idonei controlli, anche a campione, e in tutti i casi in cui sorgono fondati dubbi, sulla veridicità delle dichiarazioni sostitutive di cui agli articoli 46 e 47.*
- *2. I controlli riguardanti dichiarazioni sostitutive di certificazione sono effettuati dall'amministrazione procedente con le modalità di cui all'articolo 43* ***consultando direttamente*** *gli archivi dell'amministrazione certificante ovvero* ***richiedendo alla medesima****, anche attraverso strumenti informatici o telematici, conferma* ***scritta*** *della corrispondenza di quanto dichiarato con le risultanze dei registri da questa custoditi.*
- *3. Qualora le dichiarazioni di cui agli articoli 46 e 47 presentino delle irregolarità o delle omissioni rilevabili d'ufficio, non costituenti falsità, il funzionario competente a ricevere la documentazione dà notizia all'interessato di tale irregolarità. Questi è tenuto alla regolarizzazione o al completamento della dichiarazione; in mancanza il procedimento non ha seguito.*
- *4. Qualora il controllo riguardi dichiarazioni sostitutive presentate ai privati che vi consentono di cui all'articolo 2, l'amministrazione competente per il rilascio della relativa certificazione, previa definizione di appositi accordi, è tenuta a fornire, su richiesta del soggetto privato corredata dal consenso del dichiarante, conferma scritta, anche attraverso l'uso di strumenti informatici o telematici, della corrispondenza di quanto dichiarato con le risultanze dei dati da essa custoditi*».

- Mentre il successivo art. 72 statuisce che:
- «*1. Ai fini dell'accertamento d'ufficio di cui all'articolo 43, dei controlli di cui all'articolo 71 e della predisposizione delle convenzioni quadro di cui all'articolo 58 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, le amministrazioni certificanti individuano un* ***ufficio responsabile*** *per tutte le attività volte a gestire, garantire e verificare la trasmissione dei dati o l'accesso diretto agli stessi da parte delle amministrazioni procedenti.*
- *2. Le amministrazioni certificanti, per il tramite dell'ufficio di cui al comma 1, individuano e rendono note, attraverso la pubblicazione sul sito istituzionale dell'amministrazione, le misure organizzative adottate per l'efficiente, efficace e tempestiva acquisizione d'ufficio dei dati e per l'effettuazione dei controlli medesimi, nonché le modalità per la loro esecuzione.*
- *3. La* ***mancata risposta alle richieste di controllo*** *entro trenta giorni costituisce violazione dei doveri d'ufficio e viene in ogni caso presa in considerazione ai fini della misurazione e della valutazione della performance individuale dei responsabili dell'omissione*».

1. La soluzione 1) implica la necessità per le amministrazioni di strutturarsi in termini di interoperabilità delle banche dati *ex* artt. 50 e 58 del CAD nonché delle collegate linee guida di DigitPA[1]. Questa soluzione comporta la realizzazione (o, ove già esistenti, l'impiego) di *web services* e di un procedimento di autenticazione e trusterizzazione fra pubbliche amministrazioni.
2. La soluzione 2) implica, invece, l'onere da parte della pubblica amministrazione che riceve una dichiarazione sostitutiva di certificazione di verificarne la veridicità, imponendo di fatto la realizzazione di canali comunicativi fra le pubbliche amministrazioni che, allo stato, risultano, invece, destrutturati, spesso fuori da ogni controllo e certezza, con il rischio di un forte degrado del servizio erogato dagli atenei ai loro utenti.

-

- [1] Cfr. *www.digitpa.gov.it*

Criticità

- Alla luce del quadro normativo attualmente vigente, la soluzione precedentemente utilizzata da diversi atenei in merito al rilascio della certificazione mediante documento analogico dotato di timbro digitale, da presentarsi, poi, ad altre pubbliche amministrazioni, non è più legittimo, **in quanto ogni produzione di certificati in tale contesto risulta del tutto nulla**.

Scenari conclusivi

Dichiarazioni online

DB ENTE

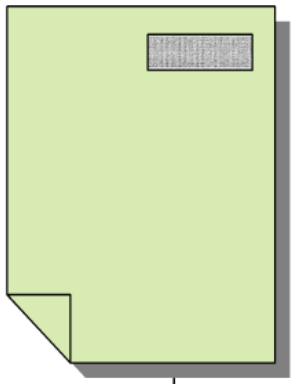
T3 Documento Inf.

Estrazione dati dal DB

T4 Contrassegno recante il tracciato record dei dati estratti

T5 Firma elettronica tecnologica (*server*) dei dati inseriti nel contrassegno

T6 Composizione e presentazione



T2 ISTANZA

T1 Autenticazione

T7 Invio

Controllo

3) Estrazione del tracciato record e verifica del certificato della firma elettronica

2) Domanda agli incaricati dell'Ente titolare delle informazioni certificate

1) Accesso diretto previa sottoscrizione di apposita convenzione

Conclusioni:

- analisi del processo e delle modifiche normative
- analisi delle tecnologie implementate nel servizio
- richiesta parere all'AGID sull'uso delle firme automatiche remote
    - modifica del CAD in sede di attuazione
- riprogettazione del processo di emissione del certificato
- ridefinizione ontologica degli oggetti coinvolti nel processo
- predisposizione della documentazione giuridica a suffragio del progetto

Grazie dell'attenzione