

## CIRCOLARE 8 febbraio 2002, n. AIPA/CR/39

(urn:nir:autorita.informatica.pubblica.amministrazione:circolare:2002-02-08;39)

---

### **Art. 14, comma 2, del decreto del Presidente del Consiglio dei Ministri dell' 8 febbraio 1999: codici identificativi idonei per la verifica del valore della chiave pubblica della coppia di chiavi del presidente dell'Autorità per l'informatica nella pubblica amministrazione.**

---

Il decreto del Presidente del Consiglio dei Ministri dell' 8 febbraio 1999 (Gazzetta Ufficiale 15 aprile 1999, n. 87), recante "Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'art. 3, comma 1, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513", ora art. 8, comma 2, del testo unico 28 dicembre 2000, n. 445, regola gli aspetti tecnici ed organizzativi relativi alla firma digitale.

In particolare, l'art. 14, comma 2, stabilisce che: "Per ciascuna coppia di chiavi sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana uno o più codici identificativi idonei per la verifica del valore della chiave pubblica".

In considerazione che, in data 4 febbraio 2002, il presidente dell'Autorità per l'informatica nella pubblica amministrazione, prof. Alberto Zuliani, ha presentato le proprie dimissioni e che, in pari data, le relative funzioni sono state assunte dal prof. Carlo Batini, è necessario provvedere alla pubblicazione dei codici identificativi relativi alla chiave pubblica della coppia di chiavi dello stesso prof. Carlo Batini costituiti dall'impronta del certificato della chiave pubblica stessa, generata impiegando ambedue le funzioni di hash previste nell'art. 3 del decreto del Presidente del Consiglio dei Ministri dell' 8 febbraio 1999.

Tali codici sono i seguenti:

- a. 1FB4 8B56 EB24 EB11 D7DB 1C2D 9F81 2E6F 291B E444, ottenuto utilizzando l'algoritmo ISO/IEC 10118-3: 1998 Dedicated Hash-Function 1, corrispondente alla funzione RIPEMD-160;
- b. 8692 FA2D 7A86 A9D3 A033 A600 5164 9B87 392E A053, ottenuto utilizzando l'algoritmo ISO/IEC 10118-3: 1998 Dedicated Hash-Function 3, corrispondente alla funzione SHA-1.

Tale certificato è stato emesso dal Centro tecnico per la rete unitaria della pubblica amministrazione in data 3 agosto 2001, con il numero di serie 3B6A 8597.

Roma, 8 febbraio 2002

Il Presidente f.f.: BATINI