AICA
Associazione Italiana per l'Informatica
ed il Calcolo Automatico

SYLLABUS

FIRMA DIGITALE E POSTA ELETTRONICA CERTIFICATA

Syllabus Versione 2.0

Informatica Giuridica
Modulo 2 – Firma Digitale e Posta Elettronica Certificata (Versione 2.0)

Il seguente Syllabus riguarda il Modulo 2 *Firma Digitale e Posta Elettronica Certificata* ed è finalizzato alla conoscenza pratica degli aspetti operativi inerenti la Posta Elettronica Certificata e la Firma Digitale.

Scopi del modulo

Il modulo Firma Digitale e Posta Elettronica Certificata richiede che il Candidato conosca le caratteristiche legali della Firma Digitale, il suo funzionamento, i certificati ed il ruolo degli enti certificatori, il suo utilizzo pratico ed il software di firma. Inoltre che il Candidato conosca le caratteristiche legali della Posta Elettronica Certificata, il suo funzionamento, i protocolli di comunicazione utilizzati, le sue caratteristiche di sicurezza ed affidabilità ed il suo utilizzo pratico.

Sezione	*Tema*	*Rif.*	*Argomento*
2.1 Le firme elettroniche	2.1.1 Firma Elettronica (FE), Firma Elettronica Avanzata (FEA), Firma Elettronica Qualificata (FEQ), Firma Digitale (FD)	2.1.1.1	Definire, secondo il disposto normativo vigente, le norme tecniche che regolano la materia della firma elettronica, avanzata, qualificata e digitale.
		2.1.1.2	Definire, secondo il disposto normativo vigente, la firma grafometrica e fornire le principali caratteristiche.
		2.1.1.3	Comprendere che la firma digitale è il risultato di una procedura informatica, detta validazione, che garantisce l'autenticità, l'integrità e il non ripudio di documenti informatici.
		2.1.1.4	Definire la differenza intercorrente tra firma elettronica qualificata e firma digitale, in riferimento all'algoritmo di crittografia a doppia chiave asimmetrica, utilizzato dalla firma digitale.
		2.1.1.5	Descrivere le differenze, tra le varie tipologie di firma elettronica, con riferimento alla validità giuridica e probatoria.
	2.1.2 Certificati digitali e Certificatori	2.1.2.1	Sapere cos'è il certificato digitale (formato, rilascio e informazioni contenute).
		2.1.2.2	Conoscere i compiti che l'AgID svolge in riferimento ai certificatori accreditati.
		2.1.2.3	Specificare che i certificatori accreditati forniscono servizi di certificazione ed emettono certificati qualificati (per la firma digitale) e certificati di autenticazione (per le carte nazionali dei servizi) per conto delle pubbliche amministrazioni.

AICA
Associazione Italiana per l'Informatica ed il Calcolo Automatico

Sezione	Tema	Rif.	Argomento
		2.1.2.4	Conoscere la procedura per richiedere la firma digitale, anche avvalendosi della tabella dei certificatori riportata sul sito dell'AgID.
		2.1.2.5	Conoscere le implicazioni che i certificati digitali revocati, scaduti o sospesi determinano sulla validità legale dei documenti informatici sottoscritti con firma elettronica qualificata o digitale.
	2.1.3 I formati di firma	2.1.3.1	Definire, secondo il disposto normativo vigente, i formati di firma consentiti (CAdES, PAdES e XAdES)
		2.1.3.2	Essere in grado di verificare la firma digitale in formato PAdES anche tramite il software di riferimento Acrobat (Professional e Reader).
	2.1.4 Software per la generazione e gestione della firma digitale	2.1.4.1	Saper generare una firma digitale tramite la crittografia a doppia chiave sia in formato CAdES (p7m) che in formato PAdES (pdf).
		2.1.4.2	Saper eseguire la verifica della firma digitale e la successiva estrazione degli oggetti firmati tramite applicazioni messe a disposizione da pubblici gestori o utilizzando l'applicazione europea Digital Signature Service (DSS), in modo conforme al disposto normativo vigente.
		2.1.4.3	Saper mantenere sempre aggiornati i prodotti di firma e verifica delle firme digitali in uso.
	2.1.5 La marca temporale	2.1.5.1	Definire, secondo il disposto normativo vigente, la marca temporale.
		2.1.5.2	Comprendere la differenza tra marca temporale e riferimento temporale.
	2.1.6 I formati della marca temporale	2.1.6.1	Sapere che il servizio di marcatura temporale si basa sull'uso delle funzioni di hashing.
		2.1.6.2	Conoscere la regola d'uso delle due differenti tipologie di formato: m7m (attached) e tsr (detached).
	2.1.7 La Time Stamping Authority	2.1.7.1	Definire il ruolo delle Time Stamping Authority (TSA).
		2.1.7.2	Comprendere la necessità di attestare una data certa sul documento informatico attraverso il servizio di marca temporale (timestamping) e definire fasi e peculiarità.

Sezione	Tema	Rif.	Argomento
	2.1.8 Generazione della marca temporale	2.1.8.1	Comprendere l'utilità della marca temporale nel caso di documenti su cui sia stata apposta una firma digitale.
		2.2.8.2	Saper marcare temporalmente un documento informatico.
2.2 La Posta Elettronica Certificata (PEC)	2.2.1 Caratteristiche principali	2.2.3.1	Determinare le caratteristiche principali della posta elettronica certificata (PEC).
		2.2.3.2	Definire la Posta Elettronica Certificata (PEC) in base al disposto normativo vigente, con particolare riferimento al concetto di busta elettronica, al significato di ricevuta elettronica di invio/ritorno e alla certezza della provenienza e destinazione.
	2.2.2 Funzionamento	2.2.2.1	Sapere cosa rappresentano: punto di accesso, punto di destinazione, punto di ricezione, punto di consegna.
		2.2.2.2	Sapere come funziona la ricevuta elettronica di invio/ritorno: dalla presa in carico all'avvenuta consegna.
		2.2.2.3	Descrivere la procedura di gestione dell'eventuale smarrimento della ricevuta elettronica.
		2.2.2.4	Saper distinguere tra messaggi firmati e cifrati.
		2.2.2.5	Saper riconoscere la provenienza e la destinazione di un messaggio PEC: certezza del mittente, certificazione dell'invio, della consegna e del ricevimento (data e ora).
	2.2.3 Garanzie ai fini legali e probatori e di sicurezza	2.2.3.1	Conoscere l'importanza di garantire la certezza del contenuto e la sua non modificabilità.
		2.2.3.2	Definire le garanzie, ai fini legali e probatori, che il servizio di posta elettronica certificata determina.
		2.2.3.3	Comprendere che le condizioni sotto le quali data e ora di trasmissione e di ricezione di un documento informatico sono opponibili ai terzi
		2.2.3.4	Conoscere le garanzie di sicurezza, a livello fisico e informatico, che i sistemi di PEC forniscono.

Sezione	Tema	Rif.	Argomento
	2.2.4 La Posta Elettronica Certificata nella PA	2.2.4.1	Specificare che le pubbliche amministrazioni provvedono a istituire e pubblicare nell'Indice PA almeno una casella di posta elettronica certificata per ciascun registro di protocollo..
		2.2.4.2	Specificare che le pubbliche amministrazioni utilizzano per le comunicazioni, tra l'amministrazione e i propri dipendenti, a posta elettronica o altri strumenti informatici di comunicazione.
		2.2.4.3	Conoscere il significato di domicilio digitale e la possibilità, riconosciuta ai cittadini dal disposto normativo vigente, di utilizzarlo come canale esclusivo di comunicazione con la PA, previa indicazione al Comune di residenza.
		2.2.4.4	Specificare che, in base al disposto normativo vigente, la PEC rappresenta, per l'interazione con la PA, una delle norme di domicilio digitale, insieme a ogni altro servizio elettronico di recapito certificato qualificato che consenta la prova del momento di ricezione di una comunicazione.
	2.2.5 La trasmissione informatica dei documenti	2.2.5.1	Determinare la validità, ai fini del procedimento amministrativo, della trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni.
		2.2.5.2	Determinare i casi in cui le comunicazioni sono valide, ai fini della verifica della provenienza.
	2.2.6 Gestione della Posta Elettronica Certificata	2.2.6.1	Sapere come e a chi richiedere e attivare una casella di Posta Elettronica Certificata (PEC).
		2.2.6.2	Sapere identificare un messaggio di PEC.
		2.2.6.3	Saper utilizzare un sistema di PEC per spedire una e-mail certificata e verificare l'avvenuta consegna e ricezione della stessa.
		2.2.6.4	Conoscere le implicazioni riguardanti l'invio di PEC ad un utente con casella PEC, ad un utente privo di PEC e viceversa.
		2.2.6.5	Sapere come si verifica un messaggio di PEC (mittente e destinatario).
		2.2.6.6	Sapere come si verificano le ricevute di invio/ritorno.
		2.2.6.7	Sapere come si verifica la Firma Digitale contenuta in un messaggio di PEC.