Scheda di approfondimento:

Tipologie di firme digitali: CAdES e modalità PAdES e Xades.

La firma digitale consiste nella creazione di un file, definito **"busta crittografica",** cioè una sorta di "pacchetto" in cui sono racchiusi più oggetti: il documento originale, la firma e certificato di autenticità di quella firma rilasciata da un certificatore fiduciario.

Il file "busta crittografica", cioè il contenitore di firma che può essere di tre tipologie: PAdES, CAdES e XAdES.

Questi tre formati appartengono alla famiglia degli appartengono alla famiglia di formati di firme digitale chiamata **AdES**, acronimo di **Advanced Electronic Signatura**, cioè firma elettronica avanzata.

COME SCEGLIERE IL FORMATO DA UTILIZZARE

La differenza tra i formati consiste soprattutto nel modo in cui si presenta il file al soggetto che vuole verificare quella firma.

1) il formato CAdES - p7m

Nel formato **CAdES, composto da C-AdES** che sta per "Cryptographic message syntax" della famiglia AdES, la busta crittografica che racchiude il documento, la firma prendono e il certificato, assumono il formato **"p7m"**

Pregi:

- può essere apposta **su qualsiasi tipo di file,** file di testo (Microsoft Word, OpenOffice Writer, semplici file di testo, etc.), fogli di calcolo (Microsoft Excel, OpenOffice Calc), file immagine (JPEG, GIF, PNG, etc.), PDF.

Difetti:

- per potere aprire la busta **"p7m**" è necessario avere a disposizione un software specifico, come DiKE, File Protector, ArubaSign, che riesca che si trova all'interno di un lettore/scrittore di smart card.
- per effettuare più firme sullo stesso documento è necessario re-imbustare in una nuova busta CAdES la prima "busta" contenente la firma con un effetto detto "matrioska".
- non è possibile aggiungere una firma grafica visibile sul documento

2) il formato PAdES - pdf

Nel formato **PAdES, composto da P-AdES** che sta per "**PDF**" della famiglia AdES, la busta crittografica assume un estensione **".pdf",**.

Nel nostro ordinamento è stata introdotta nel 2006 a seguito di un protocollo di intesa tra Adobe e l'allora CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione)
Nel 2011 la Commissione Europea nella decisione 2011/130/EU ha imposto il suo utilizzo nei documenti firmati elettronicamente nel mercato interno avendo risolto alcuni difetti della firma CAdES.

La busta PAdES è un formato particolarmente idoneo quando è necessario apporre una nuova firma al documento dopo la prima sottoscrizione digitale.

Pregi:

- non è necessario alcun tipo di software e lettore specifico per aprire la busta che si apre in PDF
- è possibile firmare un documento senza l'effetto matrioska e senza invalidare le sottoscrizioni precedentemente apposte.
- è possibile aggiungere una firma grafica visibile sul documento, oltre quella digitale, potendo quindi essere inserita nel punto desiderato del documento

Difetti:

- è possibile firmare solo PDF.

In conclusione, la busta PAdES è un formato particolarmente idoneo quando è necessario apporre una nuova firma al documento dopo la prima sottoscrizione digitale

3) Il formato XAdES - xml

Il formato **XAdES,** che sta per "**XML**" della famiglia AdES, è lo standard per la sottoscrizione elettronica dei documenti in formato XML.

Pregi:

- non necessita di imbustamento/sbustamento
- può accedere ai "metadati" , cioè quelle informazioni contenute nei tag xml, formato utilizzato per elaborazioni numeriche.
- è possibile firmare un documento senza l'effetto matrioska e senza invalidare le sottoscrizioni precedentemente apposte

Difetti:

- i file xml sono di difficile lettura.