Manual de signatura electrònica

Versió gener de 2021

Agència Balear de l'Aigua i la Qualitat Ambiental

MALLORCA: Polígon Son Rossinyol. Gremi Corredors, 10. 07009 Palma. Telèfon 971 17 76 58 Fax 971 17 76 78
MENORCA: Camí des Lloc de Monges, s/n. 07760 Ciutadella. Telèfon/Fax 971971 48 29 00
EIVISSA: Rotonda Santa Eulàlia, s/n. 07800 Eivissa. Telèfon 971 19 31 90 Fax 971 31 75 88

1 Definició

La signatura electrònica és un conjunt de dades digitals que acompanyen o que estan associats a un document electrònic i que té les següents funcions:

- Identificar el signant de manera inequívoca
- Assegurar la integritat de el document signat. Assegura que el document signat és exactament el mateix que l'original i que no ha patit alteració o manipulació.
- Assegurar el no repudi del document signat. Les dades que utilitza el signant per realitzar la signatura són únics i exclusius i, per tant, posteriorment, no pot dir que no ha signat el document.

La base legal de la signatura electrònica està recollida en la Llei 59/2003 de Signatura Electrònica i es desenvolupa en més profunditat en la secció Base legal de les Signatures. La secció també explora, sota quines circumstàncies la llei equipara la signatura electrònica a la signatura manuscrita, afegeix notes respecte a la normativa europea i fa diverses referències legals a firmes amb segells de temps i avançades.

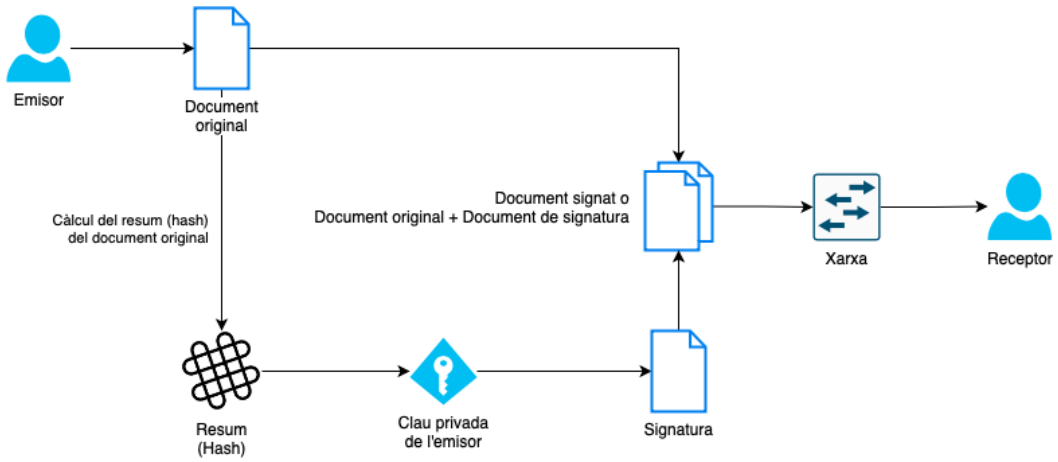
2 El certificat electrònic. La base de la signatura electrónica

Per signar un document és necessari disposar d'un certificat digital o d'un DNI electrònic.

El certificat electrònic o el DNI electrònic conté unes claus criptogràfiques que són els elements necessaris per a signar. Els certificats electrònics tenen l'objectiu d'identificar inequívocament al seu posseïdor i són emesos per Proveïdors de Serveis de Certificació, com per exemple, la FNMT (Fàbrica Nacional de Moneda i Timbre).

A l'entorn de la CAIB, els certificats electrònics s'instal·len a dins una targeta criptogràfica, però des del punt de vista legal, es tan vàlid signar amb el DNI electrònic com signar amb el certificat personal facilitat per la FNMT o amb els certificats digitals que proveu la CAIB.

3 El procés bàsic de signatura electrònica



El procés bàsic que se segueix per a la signatura electrònica és el següent:

- L'usuari disposa d'un document electrònic (un full de càlcul, pdf, una imatge, o fins i tot un formulari en una pàgina web) i d'un certificat que li pertany i l'identifica de forma unívoca.
- L'aplicació o dispositiu digital utilitzats per a la signatura realitza un resum (el resum o hash, no és més que un conjunt d'operacions matemàtiques) del document. El resum d'un document de grans dimensions pot arribar a ser tan sols d'unes línies. Aquest resum és únic i qualsevol modificació de el document implica també una modificació de l'resum.
- L'aplicació utilitza la clau privada per codificar el resum.
- L'aplicació crea un altre document electrònic que conté aquest resum codificat. Aquest nou document és la signatura electrònica.
- El resultat de tot aquest procés és un document electrònic obtingut a partir de l'original i de les claus de l'signant. La signatura electrònica, per tant, és el mateix document electrònic resultant.

4 Com signo un document?

Algunes de les preguntes que poden sorgir en el procés anterior són:

- Quina eina he d'utilitzar per signar?
- Necessito instal·lar alguna cosa al meu ordinador?
- I quan signo un formulari a internet He instal·lar alguna cosa o el meu navegador ja ho fa tot automàticament?
- Com ús el DNI electrònic des del meu ordinador? Com instal el lector de DNI?

4.1 Quina eina he d'utilitzar per signar?

Ja que estem parlant de signatura electrònica, la signatura s'ha de fer obligatòriament per mitjans electrònics i la podràs realitzar de dues formes:

- **L'aplicació AutoFirma, del Ministeri d'Hisenda i Administracions Públiques**. Aquesta aplicació la instal·lem des del departament TIC, i us la deixem configurada tal i com s'ha d'usar, tot i que és necessari saber com modificar-ne algunes opcions atès que en funció del tipus d'element a signar s'han de modificar.
- **Signar directament a internet**: Aquesta opció és usada sobretot quan signatures formularis o sol·licituds, per exemple, en la relació amb l'Administració Pública. Però també pots signar els teus propis documents a internet utilitzant el servei ofert per VALIDe. Per signar ha de descarregar-se una component que funciona sobre el mateix navegador.

4.2 Formats de signatures

4.2.1 Què són els formats de signatura?

El format de signatura és la forma com es genera el document de signatura i com es guarda o estructura la informació de signatura en el document generat.

L'existència de múltiples formats de signatura es deu a raons històriques, a com s'ha anat introduint la signatura en formats de documents ja existents i a com s'han anat afegint funcionalitats al llarg de el temps.

Un fitxer de signatura té un format que ve determinat per aquests aspectes:

- Estructura de el fitxer: formats CAdES, XAdES, PAdES, OOXML, ODF ...
- On es guarda el document original?
- Firmes amb múltiples usuaris.
- Longevitat de la signatura i segell de temps

4.2.2 Estructura de la signatura: CAdES, XAdES, PAdES, OOXML, ODF ...

Una signatura electrònica és un fitxer que conté informació sobre el document original, el signant, la data de la signatura, algoritmes utilitzats i possible caducitat de la signatura.

Com s'estructura aquesta informació (l'ordre d'aquesta informació dins de l'fitxer, les etiquetes que indiquen quan comença un camp i quan acaba, l'opcionalitat d'aquests camps, etc.) ve determinat per diferents formats:

4.2.2.1 CAdES (CMS Avançat)

És l'evolució de el primer format de signatura estandarditzat. És apropiat per signar fitxers grans, especialment si la signatura conté el document original perquè optimitza l'espai de la informació. Després de signar, no podràs veure la informació signada, perquè la informació es guarda de forma binària.

4.2.2.2 XAdES (XML Avançat)

El resultat és un fitxer de text XML, un format de text molt similar a l'HTML que utilitza etiquetes. Els documents obtinguts solen ser més grans que en el cas de CAdES, per això no és adequat quan el fitxer original és molt gran. Aplicacions com eCoFirma de el Ministeri d'Indústria i Comerç, només signen a XAdES.

4.2.2.3 PAdES (PDF Avançat)

Aquest és el format més adequat quan el document original és un pdf. El destinatari de la signatura pot comprovar fàcilment la signatura i el document signat. Amb els formats anteriors això no és possible si no s'utilitzen eines externes.

4.2.2.4 OOXML i ODF

Són els formats de signatura que utilitzen Microsoft Office i Open Office, respectivament.

L'aplicació client AutoFirma permet configurar el format a utilitzar.

4.2.3 On es guarda el document original?

Segons com es faci referències o on es guardi el document original en el fitxer de signatura, podem tenir dos casos:

4.2.3.1 El document original s'inclou en el fitxer de signatura

Avantatge: No cal guardar sempre el document original i el document de signatura perquè aquell ja està inclòs en aquest. És, per tant, un format còmode d'emmagatzemar.

Desavantatge: Si la mida de l'arxiu és elevat, es consumeix més espai d'emmagatzematge, perquè a la fi s'acaba tenint d'una banda el document original, que sempre caldrà guardar-lo, i de l'altra, la firma.

En el cas de CAdES aquestes firmes es diuen signatures implícites.

En el cas de signatures XAdES XML, l'habitual és que el document estigui inclòs en el fitxer de signatura. Parlem de signatures desenganxades (detached), envoltants (enveloping) i embolicades (enveloped) segons en quin lloc de l'propi fitxer de signatura es guardi el document original.

A la pràctica, se sol utilitzar el cas 1, que és la manera de funcionar per defecte de les aplicacions de signatura. S'obtenen fitxers de signatura més grans però, com a contrapartida, no requereix emmagatzemar l'original i un altre document a part al costat de l'de signatura.

4.2.3.2 El document no s'inclou en la signatura

En aquest cas, el document no s'inclou en el resultat de signatura o només s'inclou una referència a el lloc en què es troba perquè el document pugui ser localitzat. Per tant, s'obtenen fitxers de mida més reduïda, però, pel contrari, el document original sempre cal guardar-lo juntament amb el de la signatura.

En el cas de CAdES aquestes firmes es diuen signatures explícites.

En el cas de signatures XAdES XML, només per a les firmes desenganxades (detached), el document pot estar fora.

4.2.4 Signatures amb múltiples usuaris

En el món de el paper i de la signatura manuscrita, un document pot contenir la signatura de diverses persones:

En alguns casos, les firmes poden tenir el mateix pes o valor legal, de manera que és igual l'ordre en el que s'estampin les signatures en el document.

En altres casos, algunes signatures serveixen per ratificar o certificar altres signatures anteriors, de manera que l'ordre en el qual s'estampen les signatures és important.

L'equivalent a aquestes firmes en el món electrònic són les signatures múltiples. Atenent al criteri del nombre de signants podem tenir:

- **Signatures simples**. Són les firmes bàsiques que contenen la signatura d'un sol signant.
- **Contra-signatura**. És la signatura múltiple en la qual tots els signants estan a el mateix nivell i en la qual no importa l'ordre en què se signa. La co-signatura s'utilitza en la signatura de documents que són resultats de reunions, conferències o comitès.
- **Contra-signatura en cascada**. Signatura múltiple en què l'ordre en què se signa és important, ja que cada signatura ha de ratificar o certificar la signatura del signant anterior. La contra-signatura s'utilitza especialment en aplicacions com el Porta Signatures, en què un document ha de seguir una línia específica a través de diversos signants fins que tot el procés és aprovat.

L'aplicació de signatura AutoFirma permet els tres tipus de signatura. L'usuari pot configurar el tipus de signatura múltiple que desitja realitzar.

Annex 1. Signatura electrònica a l'Agència Balear de l'Aigua i la Qualitat Ambiental

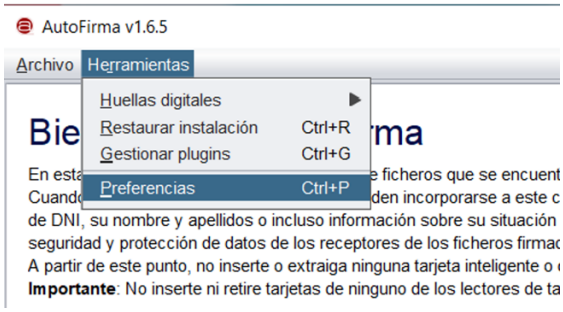
5 Annex 1. Signatura electrònica a l'Agència Balear de l'Aigua i la Qualitat Ambiental

A l'Agència Balear de l'Aigua i la Qualitat Ambiental es defineixen els següents estàndars:

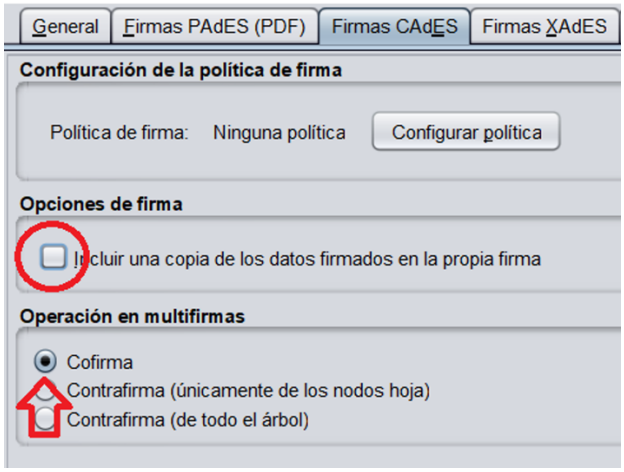
- El format de fitxers de qualsevol document, tant interns com extern, susceptible de ser signat ha de ser PDF.
- Si l'objecte susceptible de ser signat és una carpeta (del disc dur, CD, PenDrive,...) s'ha de generar un únic fitxer comprimit, en format .zip, del que es generarà l'emprempta digital, per a posteriorment signar-la.
- El format de signatura electrònica per defecte dels fitxers a signar ha de ser **CAdES**.
- La signatura electrònica **NO** ha d'incloure el fitxer original. D'aquesta forma, separant els fitxers de signatura dels fitxers de dades signats, evitam problemes amb les signatures múltiples dels documents que es crean a partir de documents PDF signats digitalment, atès que al fusionar els documents les signatures no hi estàn incloses.

5.1 Configuració d'AutoFirm@

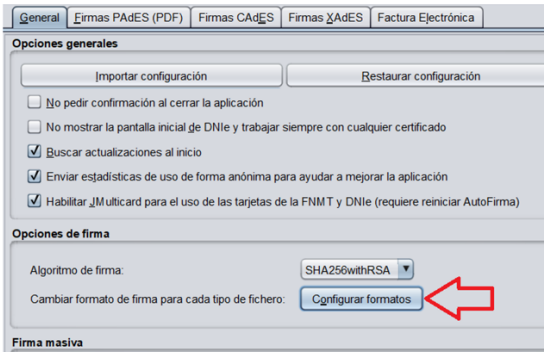
Per a configurar l'AutoFirm@ hem d'obrir l'aplicació i anar a *Herramientas -> Preferencias*.



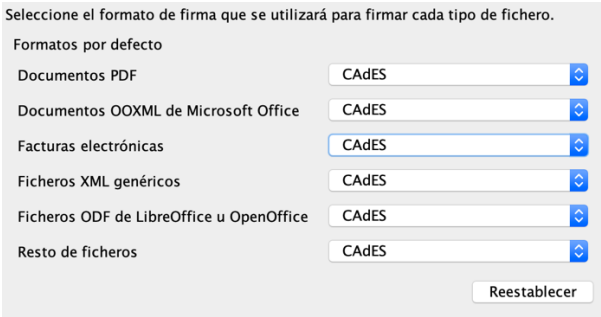
Després, a la secció Firmas CAdES desmarquem l'opció "*Incluir una copia de los datos firmados en la pròpia firma*", i marquem l'opció "*Cofirma*".



Un cop fet això, a la secció "*General*", triem l'opció "Configurar formatos".



I seleccionem el format CAdES per a tots els formats.



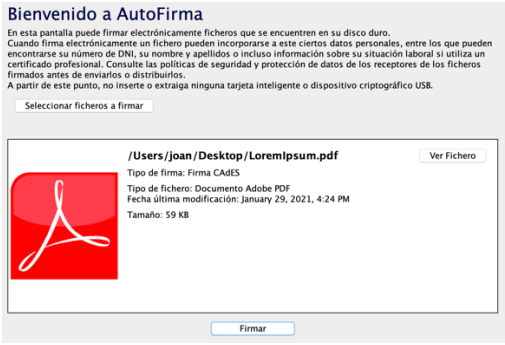
Un cop fet això, tanquem l'aplicació i la tornem a posar en marxa.

5.2 Signatura simple

Com hem vist abans, a la secció 4.2.4 existeixen signatures simples i signatures múltiples (contrasignatures i contrasignatures en cascada). A aquest manual es mostra com realitzar les signatures simples i les signatures múltiples, en la versió contra-signatura.

5.2.1 Signar documents PDF

Per a signar un document PDF, hem d'obrir l'AutoFirm@ (prèviament s'ha d'haver configurat tal i com s'indica al punt 5.1) i seleccionem el fitxer a signar.



Al seleccionar firmar ens demanarà on volem guardar el document de signatura. Com a recomanació s'indica anomenar el fitxer de signatura igual que el fitxer, però amb l'extensió .csig.

RECORDATORI

Aquest format de signatura implica que s'han de guardar dos fitxers. Per una banda el fitxer PDF, i per l'altra el fitxer de la signatura.

Per a comprovar les signatures dels documents s'ha de fer amb l'aplicació de **VALI**dació de signatura i certificats online i **De**mostrador de serveis de @firma (o VALIDe) de. Consulteu la secció 5.5 per a veure com fer-ho.

5.2.2 Signar documents .zip

Per a signar documents .zip primer hem de calcular l'emprempta digital del document .zip. Un cop s'ha obtingut el fitxer que conté l'emprempta digital del document, aquest s'ha de signar com si es tractés d'un fitxer PDF. A la següent secció es mostra com calcular l'empremta digital d'un document.

Per tant, un cop realitzat el procediment, en aquest cas obtindrem 3 fitxers.

- El fitxer .zip original
- El fitxer que conté l'empremta digital (generalment un .hexhash)
- El fitxer de signatura digital (igual que al cas del document PDF)

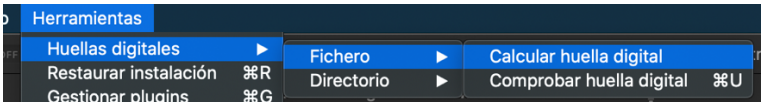
Els objectius de generar documents .zip per tal de poder-los signar son bàsicament dos:

- A la plataforma de l'estat, a les seus electròniques dels ajuntaments, per mail i, en general, a qualsevol plataforma que ens permeti fer l'enviament de la documentació en format digital les mides dels fitxers a enviar estan limitades. Generar un fitxer .zip, calcular la seva empremta digital i signar l'emprempta ens permet enviar únicament el fitxer de signatura i el fitxer d'emprempta (que en cap cas poden superar els 2Mb) i enviar per correu ordinari un PenDrive o un DVD amb la informació original, evitant així els límits de les plataformes web.
- En cas de tenir molts de documents, siguin del tipus que sigui ens permet fer una signatura del lot sencer, evitant feina de signar.

5.2.3 Calcular l'emprempta digital

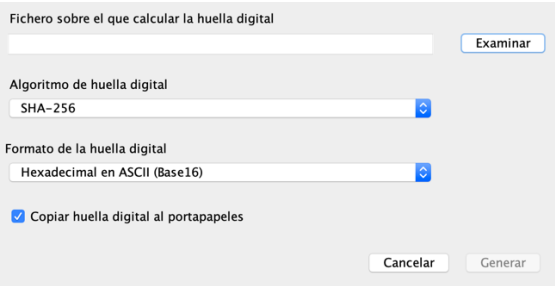
Per a calcular l'emprempta digital d'un arxiu obrim l'AutoFirma, i anem a:

- *Herramientas -> Huellas digitales -> Fichero -> Calcular huella digital*.

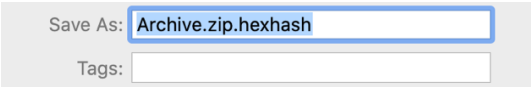


Al quadre de diàleg que se'ns obrirà senzillament escollim el fitxer del que volem calcular-ne l'empremta, i els formats que venen configurats per defecte, que són:

- Algoritme: SHA256
- Format: Hexadecimal en ASCII



Un cop fet això ens demanarà on volem emmagatzemar el fitxer d'emprempta digital i llestos.



Com s'ha dit abans, aquest fitxer es pot signar com si d'un PDF es tractés i d'aquesta forma ja tindrem els tres fitxers. Per una banda l'original i per altra, el d'emprempta digital i el de signatura digital.

5.3 Signatura múltiple

La signatura digital múltiple permet que vàries persones signin un mateix document. Aquesta es pot fer de vàries formes, però el format que s'ha escollit a l'Agència Balear de l'Aigua i la Qualitat Ambiental, com ja hem dit, és el de Contra-Signatura.

Aquest procediment implica que totes les signatures tenen el mateix pes a dins el document, i que per tant, és indiferent l'ordre de realització de les signatures.

Com a resultat s'obté igualment el fitxer original, juntament amb un fitxer de signatura.

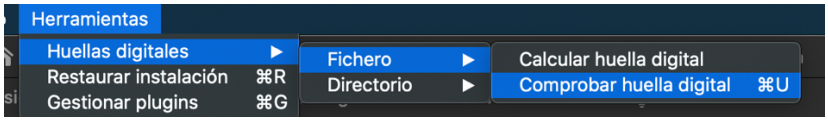
Aquest procediment d'inicia de forma idèntica al que s'explica al punt 5.2.1 d'aquest document, on s'explica com signar PDFs. És a dir, un usuari signa el document inicialment. Quan ja es tè el fitxer de signatura, els següents usuaris no signen el document original, sinó que signen el document de signatura. D'aquesta forma, les signatures es sumen al document de signatura original.

5.4 Comprovar l'emprempta digital

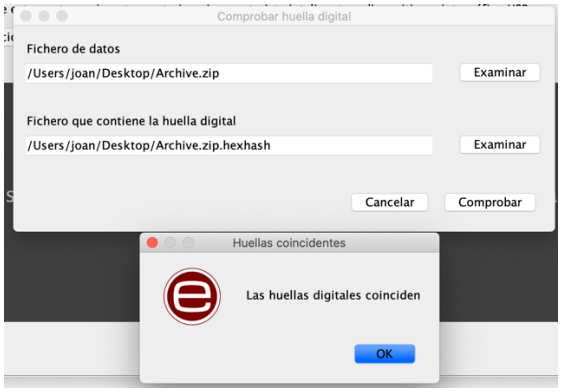
Aquest procediment és important, atès que és el que s'ha de dur a terme en rebre documents per correu ordinari dels quals ens han enviat la signatura digital. Per exemple, això pot passar en rebre documents de projectes constructius de mides elevades.

El procediment és molt senzill. Primer obrim l'AutoFirma. Després anem a :

- *Herramientas -> Huellas digitales -> Fichero* o *Directorio* (segons correspongui) -> *Comprobar huella digital*.



Al quadre de diàleg que se'ns obrirà ens demanarà el fitxer o directori a comprovar, i el fitxer de l'empremta digital.



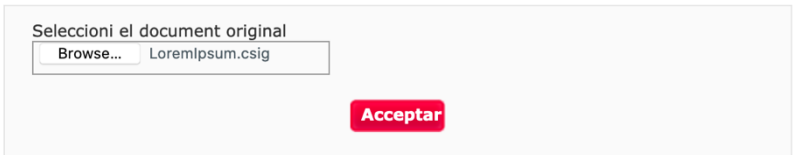
Un cop triats, triem "Comprobar" i ens dirà si l'emprempta digital es correspon amb l'emprempta digital del fitxer seleccionat, i per tant, podem assegurar que el contingut no no s'ha modificat posteriorment al càlcul de l'emprempta.

5.5 Comprovar les signatures de documents

Com s'ha mencionat abans la comprovació de les signatures electròniques s'ha de fer amb l'eina VALIDe. Aquesta aplicació està disponible a https://valide.redsara.es/.

Per a validar una signatura necessitem el fitxer original i el fitxer de signatura. Un cop a la web, triem "Validar Signatura".

Introduïm les dades que se'ns demana i el codi CAPTCHA.



I com a resultat ens indicarà si la signatura és correcta o no, i ens donarà l'opció de descarregar un justificant de la comprovació, que és com aquest.

Lorem Ipsum

"Neque porro quisquam est qui dolorem ipsum quia dolor sit amet, consectetur, adipisci velit..."
"There is no one who loves pain itself, who seeks after it and wants to have it, simply because it is pain..."

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nulla pulvinar, sem in commodo ultrices, turpis nisl suscipit ante, ut suscipit est diam laoreet sem. Vestibulum a diam at leo imperdiet lacinia vitae quis nunc. Mauris feugiat lorem commodo magna ornare finibus. Nullam faucibus, sem id laoreet scelerisque, enim libero volutpat tellus, quis condimentum odio mi in ante. Integer tincidunt pellentesque dolor, in faucibus purus faucibus vel. Aliquam erat volutpat. Mauris fringilla, quam eget tempor faucibus, est dui dictum erat, quis tempus justo massa eu lectus. Donec tempus, ipsum sit amet dapibus pellentesque, nisl dui dignissim magna, vehicula blandit lectus nisi quis metus. Nullam non scelerisque libero. Pellentesque fermentum convallis lorem. Morbi ultrices massa et tellus rhoncus, a luctus urna malesuada. Phasellus in est vestibulum, ornare turpis ut, dictum felis. Vivamus eros felis, efficitur quis nibh a, blandit scelerisque metus. Duis ac justo mi. Curabitur nisi risus, dictum ac posuere ut, imperdiet in ipsum.

Donec imperdiet interdum facilisis. Praesent faucibus blandit nulla, at hendrerit libero fringilla id. Nunc a accumsan nunc, ut lacinia justo. Nunc sit amet libero eu lorem ullamcorper luctus. Integer porta non quam ac venenatis. Pellentesque in ultricies ligula. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Vivamus gravida placerat nulla.

Vivamus rutrum in orci a pretium. Etiam rhoncus pharetra magna vel sollicitudin. Morbi luctus mi ut lobortis faucibus. Cras nisl eros, vulputate sit amet gravida id, tempus vitae ante. Donec congue metus orci, ac pharetra ligula auctor non. Nullam elementum dolor neque, nec imperdiet mauris consectetur sed. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque maximus lorem et eros tempus tincidunt non eget est. Donec elit felis, imperdiet sit amet auctor a, placerat convallis arcu. Curabitur vitae posuere tellus. Mauris felis sapien, accumsan vel laoreet ut, pharetra sit amet purus. Sed vel sem dolor. Curabitur a metus sodales, lacinia nulla sit amet, pellentesque mi.

Nullam pellentesque augue ut lorem rutrum maximus. Duis luctus turpis at ligula lacinia mattis. Aenean id urna eget tortor varius maximus. Morbi ac magna vulputate, porttitor sem quis, sagittis velit. In eget dui id erat pretium vestibulum eget eget elit. Donec sit amet lectus maximus, rhoncus erat a, consectetur elit. Nulla a enim quis felis congue pretium. Proin tempor sagittis tempor. Nunc imperdiet, sem pretium egestas tempor, urna est accumsan lectus, dignissim consectetur quam leo sit amet orci. Donec sodales arcu lorem, vel tincidunt sem venenatis sit amet. Sed sit amet vestibulum mauris. Curabitur consequat purus sed venenatis egestas. Integer gravida massa congue, congue ipsum et, lacinia erat. Proin dapibus maximus lorem ac semper. Phasellus rhoncus sem sed posuere porta.

Mauris eu mauris eleifend sem facilisis laoreet. Nunc ornare pulvinar eros, sed feugiat ipsum viverra vel. Quisque enim ex, iaculis non semper quis, pharetra vel nisi. Cras quis diam sollicitudin tortor tristique laoreet. Vestibulum ac rutrum lectus, non sollicitudin elit. Donec posuere leo sed purus hendrerit, sit amet dictum arcu varius. Morbi sed lobortis nisl. In accumsan, tellus nec maximus luctus, ante leo interdum nisl, eget mollis turpis tortor non elit. Aenean euismod non mauris at hendrerit. Etiam non semper felis.

Mauris eget iaculis ex. Proin ut nulla vel ipsum fermentum maximus. Donec quis efficitur lacus. Aliquam erat volutpat. Maecenas turpis magna, pellentesque a turpis quis, ultrices cursus orci. Donec elementum scelerisque dolor vel volutpat. Maecenas viverra gravida sapien, quis commodo nibh blandit sit amet. Ut fringilla erat urna, sit amet accumsan leo egestas nec. Aenean varius lacinia nunc vitae interdum. Mauris posuere enim ut magna suscipit malesuada. Praesent eget vehicula lectus.