Entre la identitat real i la digital

Ricardo González Mas

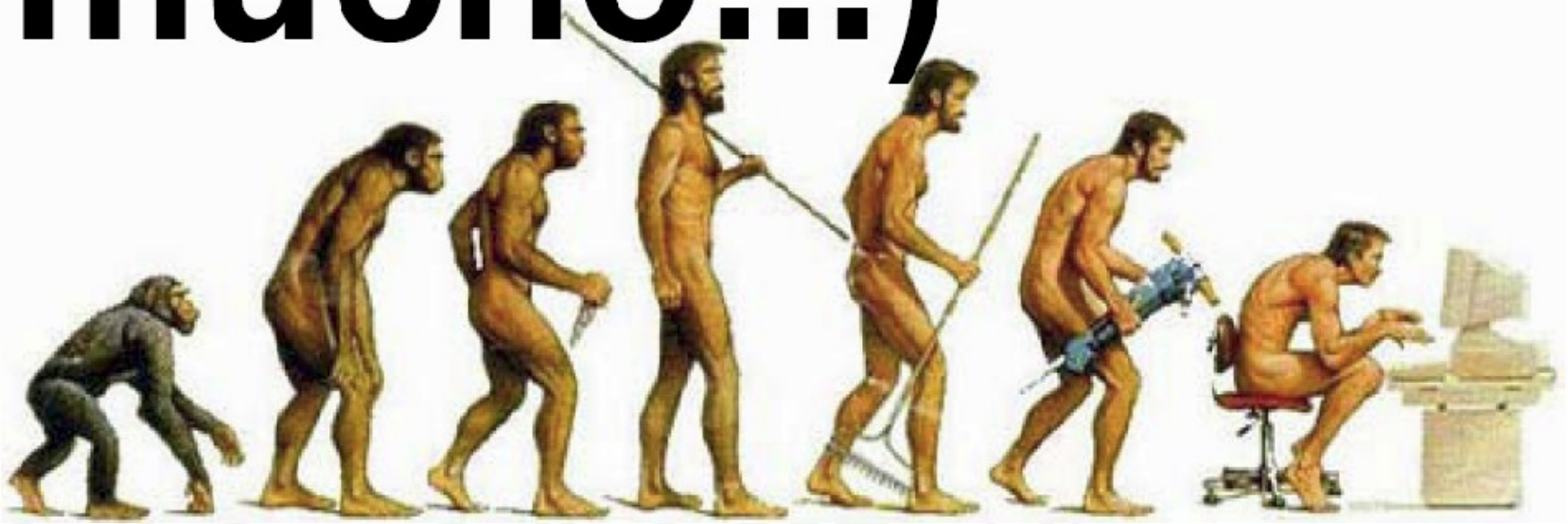
18 de Juny de 2013

Valls

Continguts

- Societat de la Informació
- Criptografia
- DNI
- Conclusions

La tecnología evoluciona (y mucho...)



Societat de la Informació

"Societat de la informació és un estadi de desenvolupament social caracteritzat per la capacitat dels seus membres (ciutadans, empreses i administracions) per obtenir i compartir qualsevol informació de forma instantànea, desde qualsevol lloc i en la forma que es vulgui (Castells 1998)"

Ajuntament de Valls

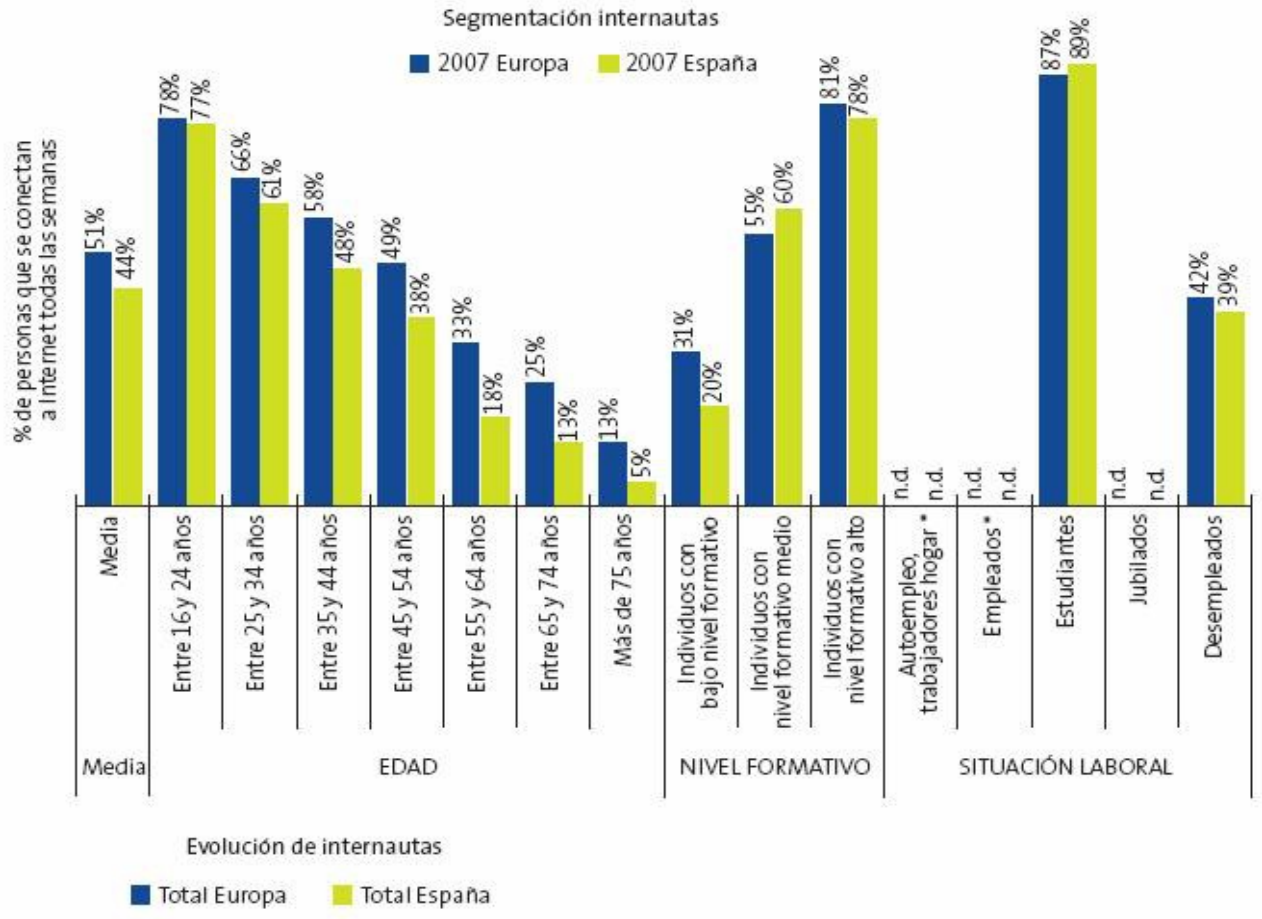
Societat de la Informació

- Elements
  - Usuaris: Persones / Organitzacions que accedeixen als continguts a través de les infraestrutures (infoestructures)
  - Infraestructures: Mitjans tècnics que fan possible l'accés remot als continguts
  - Continguts: Informació, productes o serveis als que es pot accedir sense necessitat de desplaçar-se obligatòriament a un lloc determinat.

Societat de la Informació

- Algunes Dades d'Interés

Figura 1-5. USUARIOS DE INTERNET (UE-27). PARTE 2.



Ajuntament de Valls

Societat de la Informació

- Internet com a producte massiu d'ús de TIC.
- Generació d'usuaris que demanen relacionar-se a través de la xarxa de forma avançada.
- Adequació dels mecanismes d'acreditació de personalitat a la nova realitat.
  - Acreditar electrònicament la identitat d'una persona
  - Signar digitalment documents electrònics, dotant-los de validesa jurídica equivalent a la signatura manual
  - Assegurar la integritat de les dades que s'estan comunicant

Ajuntament de Valls

Criptografia

La seguretat és necessaria

- Mecanismes d'acreditació de la personalitat dins la realitat de la Societat de la Informació
- Existència de garanties jurídiques en les transaccions electròniques (comercials com amb l'administració)

A Internet, ningú sap que ets un gos

1993 New Yorker

Criptografia

- Concepte:
  - Criptografia és un terme d'origen grec que prové dels mots krypto ("amagar") i grapho ("escriure"). Podem dir que la criptografia és la ciència i l'estudi de l'escriptura secreta.
- Per a què serveix?
  - Protegeix les dades que viatgen per un mitjà de comunicació o guardades en un sistema informàtic, des de dos vessants:
    - **Secret o privadesa:** preserva la confidencialitat de les dades.
    - **Integritat o autenticitat:** impedeix la modificació no autoritzada de les dades.

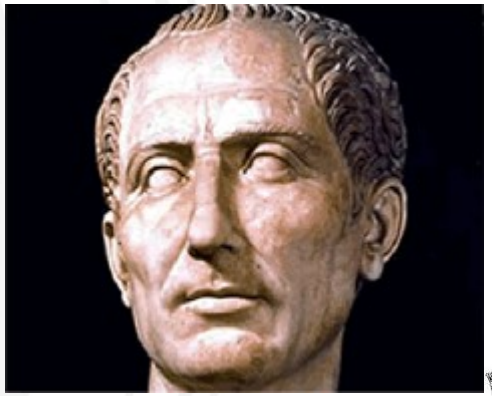
Criptografia

- Evolució: Xifratge de Cèsar (segle I a.C)
  - Es desplacen les lletres n llocs; la clau és n

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
X	*Y*	*Z*	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*

ZBXOXRDRPQX
Clau: número 3
CESARAUGUSTA

Problema: Manteniment del Secret
Secreto de muchos, secreto de ninguno



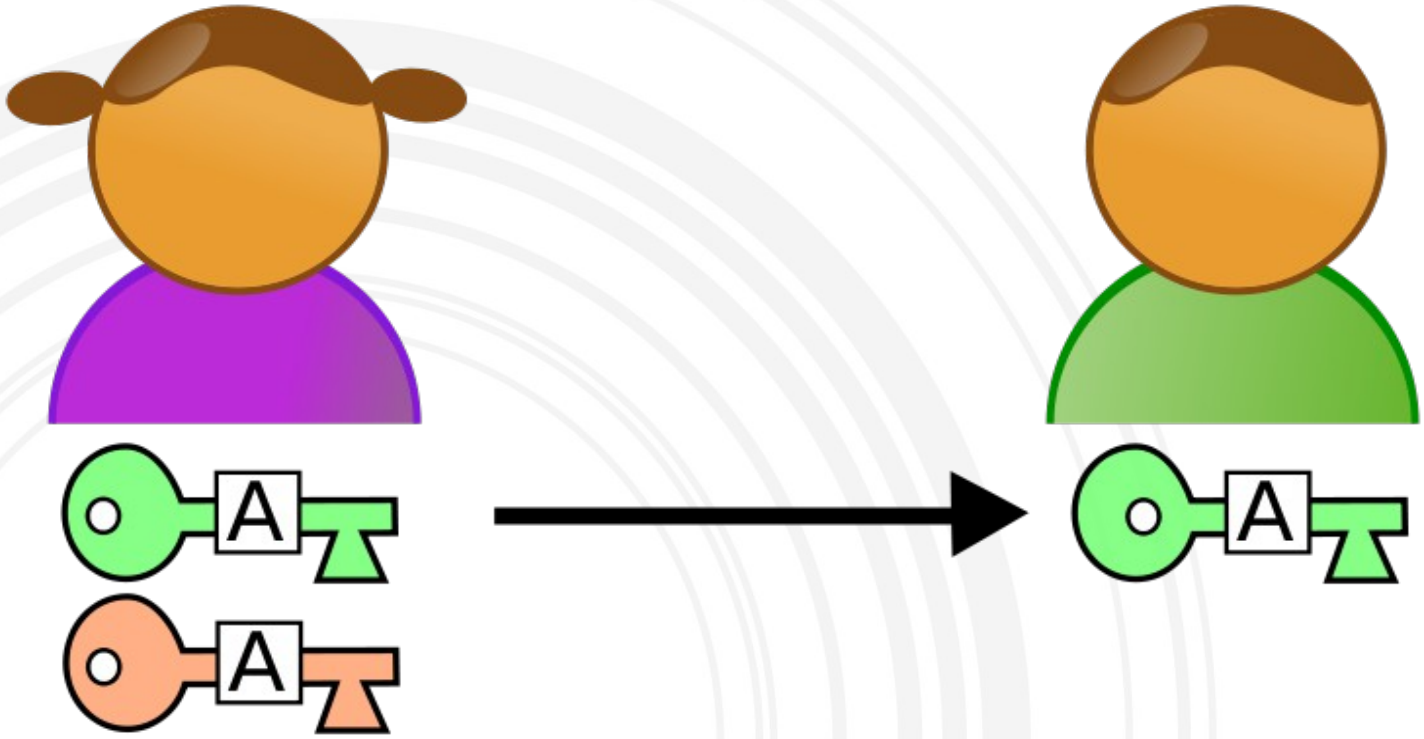
Ajuntament de Valls

Criptografia

Evolució històrica

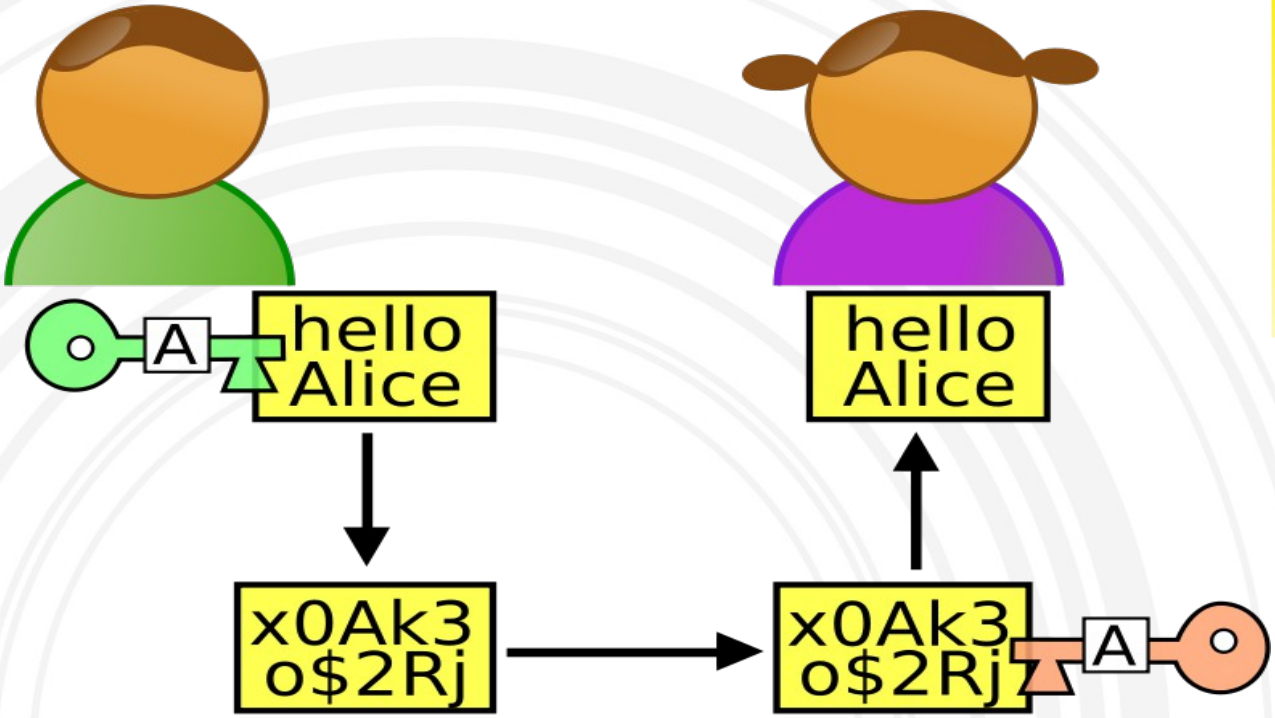
- L'aparició de l'ordinador provoca una revolució científica de les tècniques criptogràfiques.
- Claude Elwood Shannon, matemàtic nord-americà l'any 1949 va iniciar l'era de la **criptografia de clau compartida**.
- Whitfield Diffie i Martin Hellman, l'any 1976 van demostrar que era possible la comunicació secreta entre dues parts sense transferència de clau. Van iniciar l'època de la **criptografia de clau pública**.

Criptografia: Model de clau pública



1a etapa: L'Anna genera dues claus. La clau pública (verda), és la que envia a en Pere. La clau privada (vermella) és la que ella conserva sense donar-la a ningú.

Criptografia: Model de clau pública



IDEA

Si en un determinat moment, B decideix contestar de forma segura:

** Ara, B utilitzarà la clau pública d'A (receptor en aquest cas), per xifrar-li el missatge.*

IDEA

** Quan A el rebi, utilitzarà la seva clau privada (A), coneguda només per ell, per tal de desxifrar-lo.*

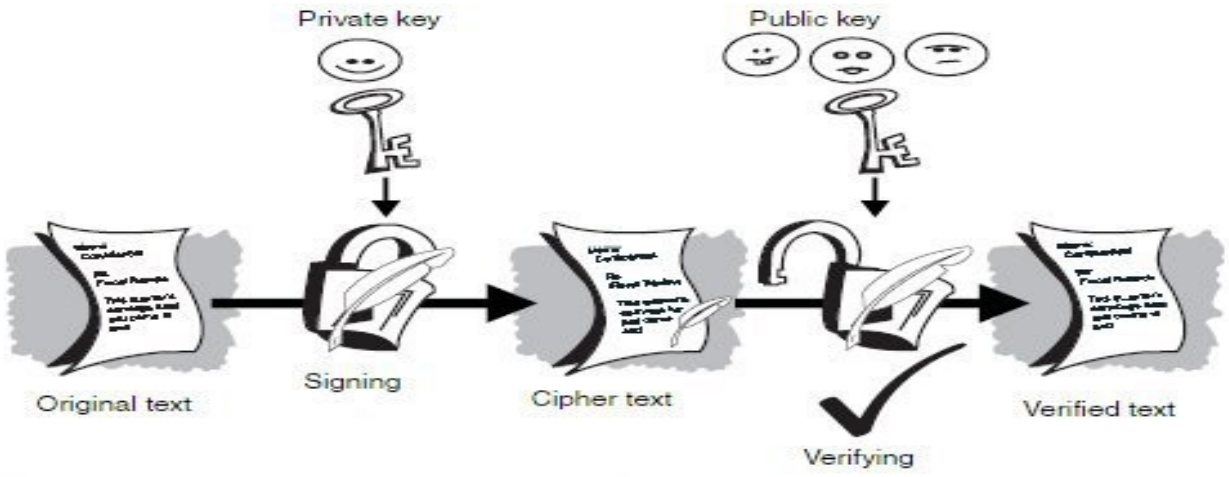
Amb aquest esquema, per cada missatge xifrat, només pot haver-hi un sol receptor.

2a i 3a etapes: En Pere xifra el missatge amb la clau pública de l'Anna, i li envia el text encriptat. L'Anna desxifra el missatge gràcies a la seva clau privada.

Ajuntament de Valls

Criptografia: Signatura Digital

- Basada en la criptografia de clau pública
- Tres motius per usar-ho
  - **Integritat**: Emissor i receptor voldran estar segurs que el missatge no s'ha alterat durant la transmissió
  - **No-repudi**: A no pot negar haver enviat el missatge a B perquè està signat amb la clau privada de A que només coneix ell
  - **Confidencialitat**: Garantida



Criptografia: Certificat Digital

- Necessitat de certificar la identitat dels participants d'una conversa que utilitza criptografia de clau pública o asimètrica.
- Un Certificat Digital és un document digital.
- Una autoritat de certificació garanteix la vinculació entre la identitat d'un subjecte o entitat i la seva clau pública.
- Autoritats

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

dni electrónico

CATCert
Agència Catalana
de Certificació

Ajuntament de Valls

DNI: Identifica al ciutadà

- Es un servei públic gestionat en exclusiva pel Cos Nacional de Policia (fa més de 60 anys)
- Les Bases de Dades que suporten la gestió del Dni es troben sota la responsabilitat de la DGP
- Característiques
  - Acredita de forma inequívoca la identitat del titular
  - Es un element present en la majoria de les relacions dels ciutadans i amb l'administració.
  - És l'únic document d'ús generalitzat en tots els àmbits a nivell de tot el territori espanyol
  - La seguretat es configura com un factor essencial en el document nacional d'identitat
  - Les dades expressades en el document, corresponen exactament amb les del seu titular.

DNI

- Evolució

DNI-E

- Llei 59/2003, de signatura electrónica
- Reial Decret 1553/2005, que regula el DNIe

Ajuntament de Valls

DNI

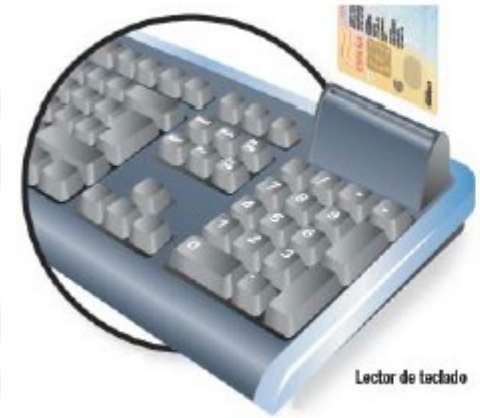
- Informació Digital
  - Certificat electrònic per autenticar la personalitat del ciutadà
  - Un certificat electrònic per a signar electrònicament (validessa jurídica)
  - Certificat de l'Autoritat Certificadora
  - Claus per a la seva utilització
  - L'empremta dactilar
  - Fotografia digital
  - Signatura manuscrita digitalizada
  - Dades de filiació del ciutadà

Característiques DNI-E

- Basat en els estandards
  - PKCS#1-sha256WithRSAEncrytion
  - X.509 Public Key Infrastructure
- Peculiaritats
  - Té dos parells de claus públiques y privades
    - Certificat digital d'autenticació
    - Certificat digital de signatura
  - Els dos certificats es troben al xip
    - Les claus privades no poden sortir de la tarjeta
  - Autoritats de Certificació: Ministerio del Interior, DGP
  - Autoritats de Validació: MAP, FNMT

Com usar el DNI-E?

- Elements hardware i software
  - Hardware
    - Un Ordinador personal (Intel -a partir de Pentium III- o similar).
    - Un lector de tarjetes intel.ligents que cumpleixi la ISO-7816.
      - Integrats al teclat, PCMCIA, lector usb



Ajuntament de Valls

Com usar el DNI-E?

- Elements hardware i software
  - Software
    - Sistema Operatiu.
      * Microsoft Windows ("Microsoft Windows (2000, XP y Vista)")
      * Linux / Unix
      * Mac
    - Navegadors
      * Microsoft Internet Explorer (versión 6.0 o superior
      * Mozilla Firefox (versión 1.5 ó superior)
      * Netscape (versión 4.78 o superior)

Ajuntament de Valls

Com usar el DNI-E?

- Elements hardware i software
  - Software
    - Controladors / Mòdulos criptogràfics
      - Serveixen per interactuar de manera adient amb la informació criptogràfica de la tarjeta
      - En entorns Windows: Servei "Cryptographic Service Provider" (CSP).
      - En entorns Unix / Linux / Mac: Mòdul criptogràfic PKCS#11
    - Eines per al canvi del Pin
    - www.dnielectronico.es/descargas

Distribució del DNI-E

- Inici: Març 2006
- A Juny de 2007 s'havien distribuït 700000 DNIe
- Estat espanyol situat a l'avantguardia tecnològica mundial
- Actualment 9000000 de DNI-E tramitats
- Aproximadament 35 milions de ciutadans majors d'edat

Serveis del DNI-E

- Serveis DNI-e de la Administración General del Estado
  - AEAT, Seguretat Social
- Serveis DNI-e de les Comunitats Autònomes
- Serveis DNI-e de l'Administració Local
  - Ajuntaments, Diputacions
- Altres Organismes Públics
  - Correos, Registro de la Propiedad
- Sector Privat
  - Caixes i Bancs

Ajuntament de Valls

Serveis Administració Local

- La llei 11/2007 (Llei d'Accés Electrònic dels Ciutadans als Serveis Públics) diu que tothom té dret a realitzar qualsevol tràmit amb l'administració de forma totalment telemàtica.
- Pla d'implantació completa d'aquests serveis
  - Instància general
  - Queixes/suggeriments/incidències
  - Canvi de domicili
  - Domiciliació de tributs
  - Recollide mobles i trastos vells
- A través del portal www.valls.cat
  - http://www.ajvalls.org/aoc/index.asp?doc=tramits&ext=htm

Noves Aplicacions

- Realitzar compres signades a través d'Internet
- Fer tràmits complets amb les Administracions Públiques
- Realitzar transaccions segures amb entitats bancaries
- Accés a edificis
- Utilitzar de forma segura el nostre PC
- Participar en converses per internet assegurant que l'interlocutor es qui diu ser

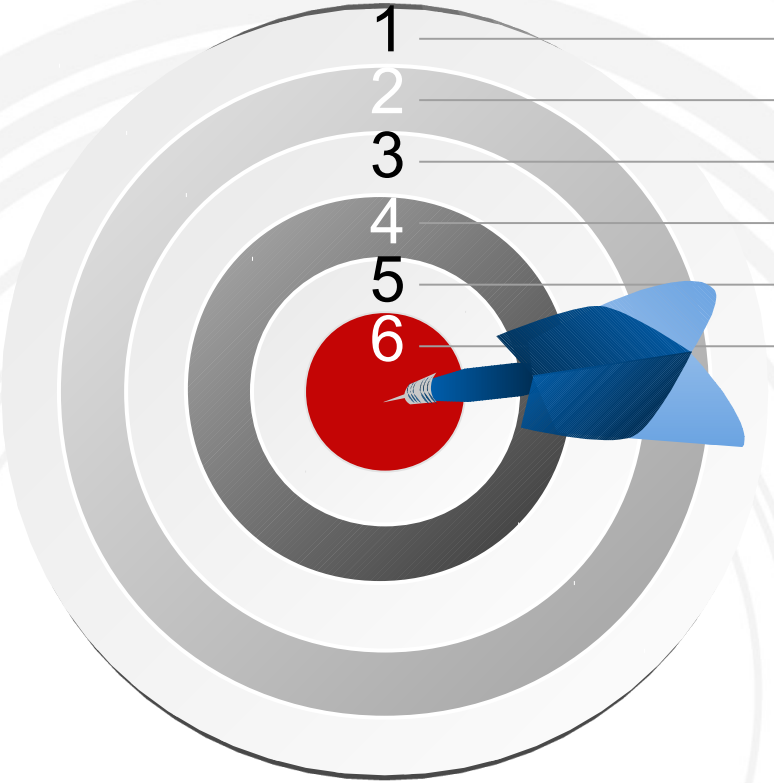
Inhibidors en el desenvolupament del DNIe

- Ausencia de massa crítica suficient
- Temps d'adopció massa lents
- Poc desenvolupament de serveis a Internet
- Poca exigència de serveis a Internet
- Poques signatures electròniques
- Poc estímul per tenir signatura electrònica

Reflexions

- L'adopció del DNIe generarà oportunitats de valor pels ciutadans i les empreses
  - implantació generalitzada de la Societat de la Informació
- L'Administració ha d'exercir un paper de lideratge
  - invertir esforços per accelerar el desplegament
- Necessària implicació activa del sector privat
  - desenvolupar nous serveis que explotin les potencialitats del DNIe

Reflexions - Desenvolupament



L'usuari CONEIX els serveis disponibles
L'usuari DISPOSA de mitjans
L'usuari NECESSITA d'aquest servei
L'usuari USA el servei per primer cop
L'usuari està SATISFET amb el resultat
L'usuari RECOMANA l'ús del servei

Ajuntament de Valls

Regidoria de Tecnologies de la Informació i Comunicacions

Conclusions

- Implantació del DNIe ha estat atrevida
- DNIe adaptada als standars internacionals
- És un projecte a mig plaç, que es completarà en 4 o 5 anys
- Grau d'utilització baix
- S'ha d'incrementar el nombre d'aplicacions i serveis, especialment en l'àmbit local
- Les entitats privades han d'oferir serveis

Gràcies

- Preguntes, aclariments dubtes, comentaris?

L'únic constant és el canvi

Heraclito de Éfeso