Sistemas de información fiables y valiosos
Valencia Chapter

V Ciclo de Conferencias ISACA
en la ETSINF

La firma electrónica: especialización y oportunidades profesionales

Nacho Alamillo Domingo, CISA, CISM, ITIL-F
Director de investigación de ISACA Valencia
Director general de Astrea

Contenidos

- Firma electrónica y servicios de confianza
- Normas y estándares aplicables.
- Especialización y oportunidades profesionales.
- La perspectiva del desarrollador.
- La perspectiva del auditor.

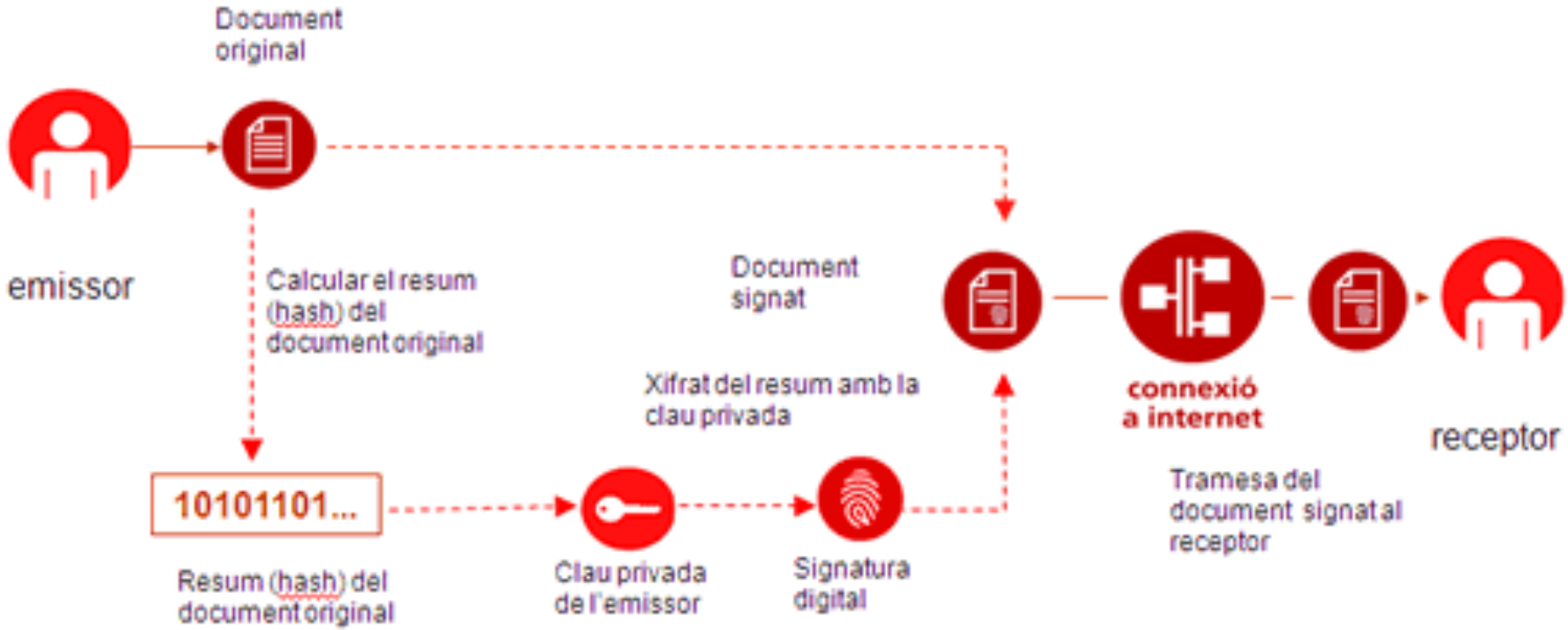
Firma electrónica y servicios de confianza – 1

- En general, la sociedad de la información precisa, para existir, un nivel mínimo de "seguridad" y de "confianza".
- ¡Somos humanos, aunque nos proyectemos al entorno electrónico! La actividad electrónica, como cualquier otro entorno nuevo, precisa referentes con el mundo «real»:
  - La «Identidad electrónica»,
  - La «Capacidad de actuación electrónica»,
  - La «Firma electrónica»,
  - Las «Evidencias electrónicas» de los actos.
- No se trata de una tecnología en concreto, sino de una precepción social, con una construcción adecuada del riesgo individual y colectivo.

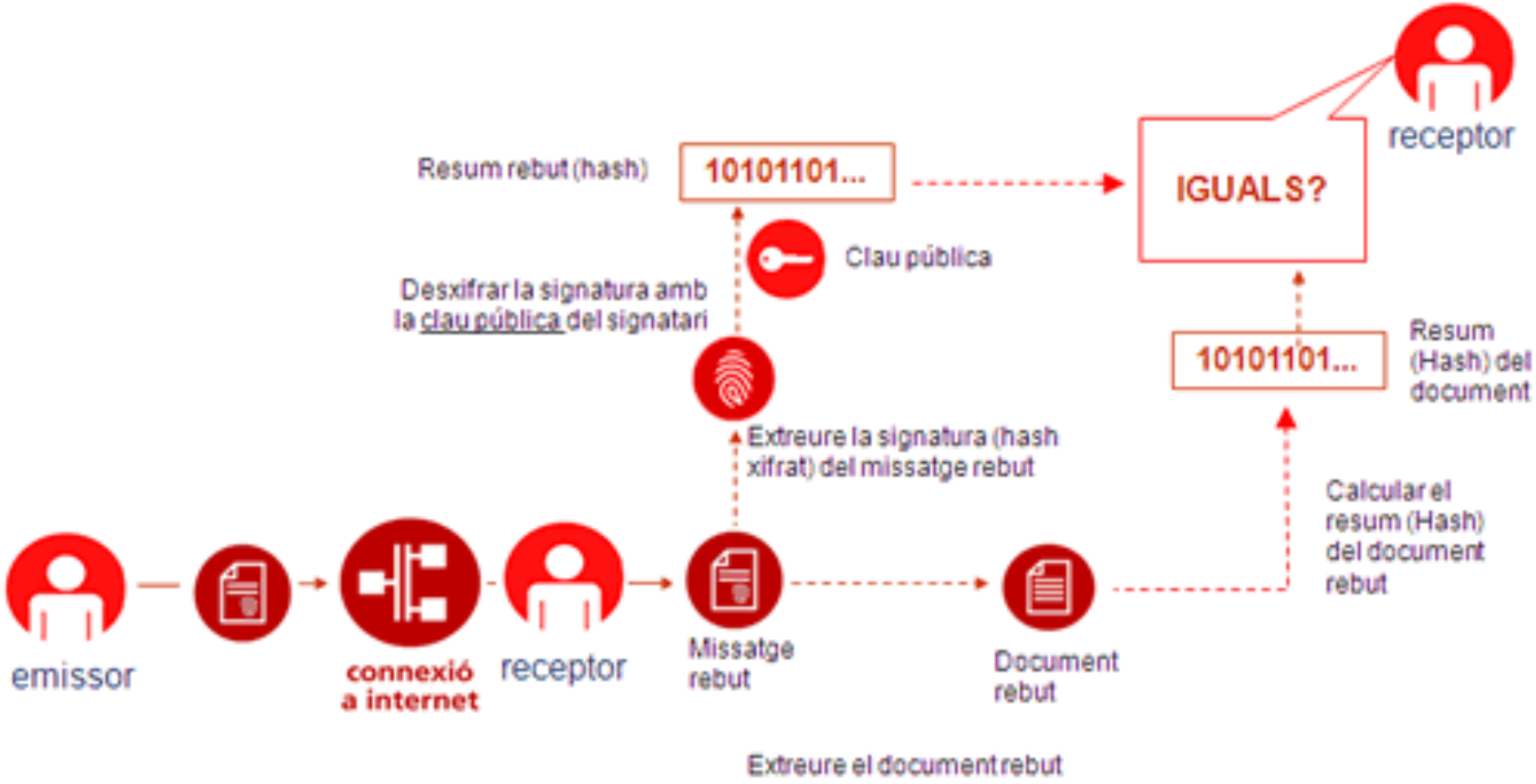
Firma electrónica y servicios de confianza – 2

- Servicios de confianza electrónica:
  - Autenticación electrónica.
  - Firma electrónica (persona física).
  - Sello electrónico (persona jurídica).
  - Sellado de fecha y hora.
  - Archivo seguro.
  - Remisión electrónica de documentos.
  - Autenticación de sitio web.
  - Autenticación de código ejecutable.
- Regulados parcialmente por Ley 59/2003, de 19 diciembre, y leyes sectoriales.
- Propuesta de Reglamento europeo sobre identificación electrónica y servicios de confianza en el mercado interior.

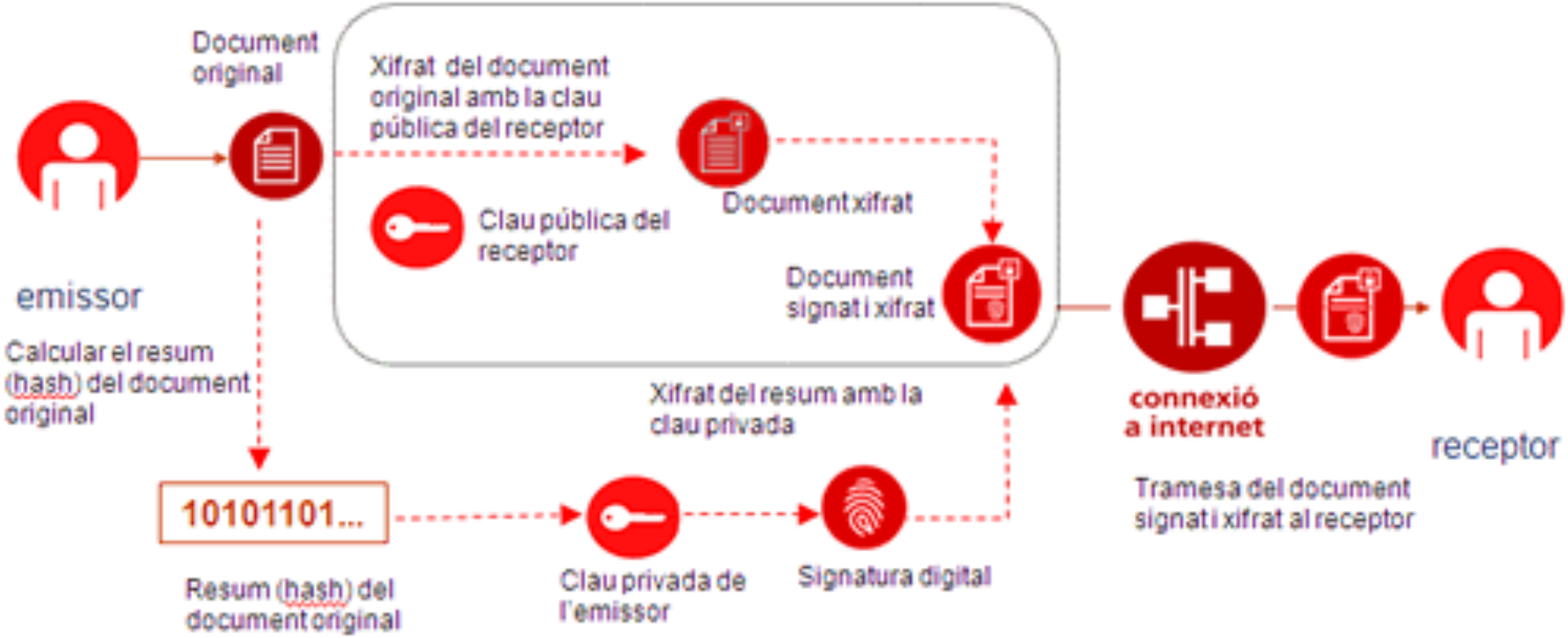
Firma electrónica y servicios de confianza – 3



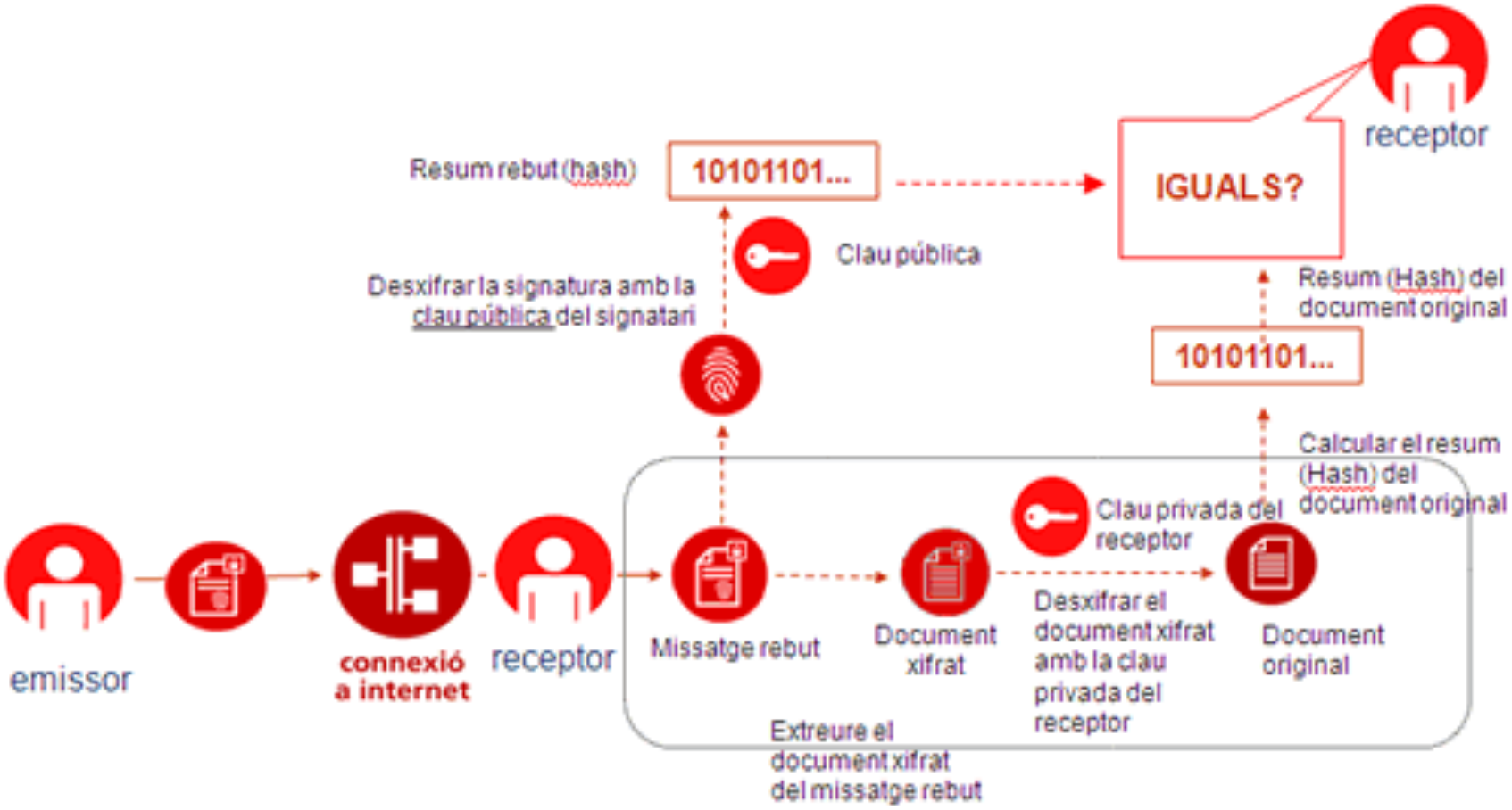
Firma electrónica y servicios de confianza – 4



Firma electrónica y servicios de confianza – 5

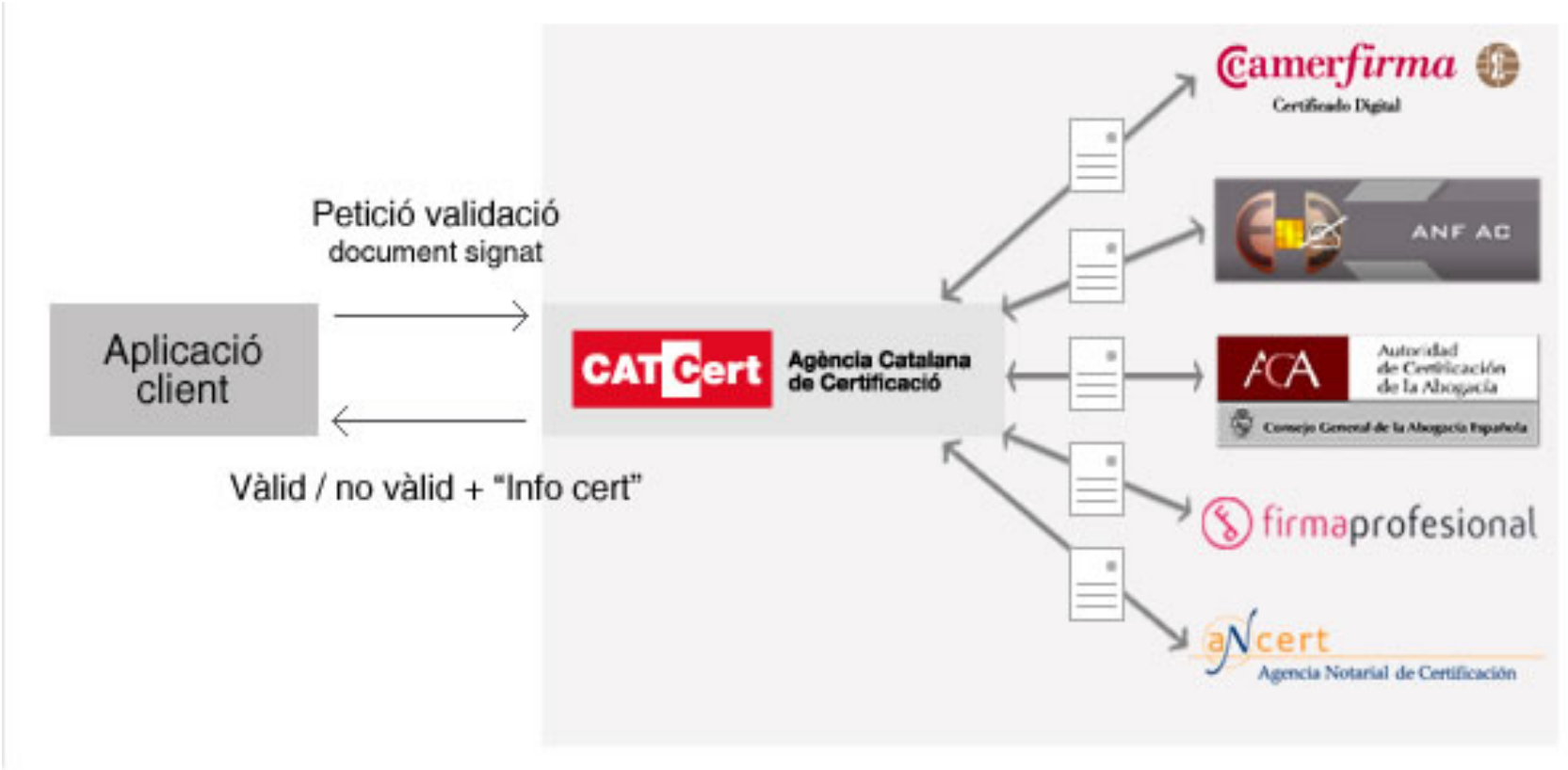


Firma electrónica y servicios de confianza – 6

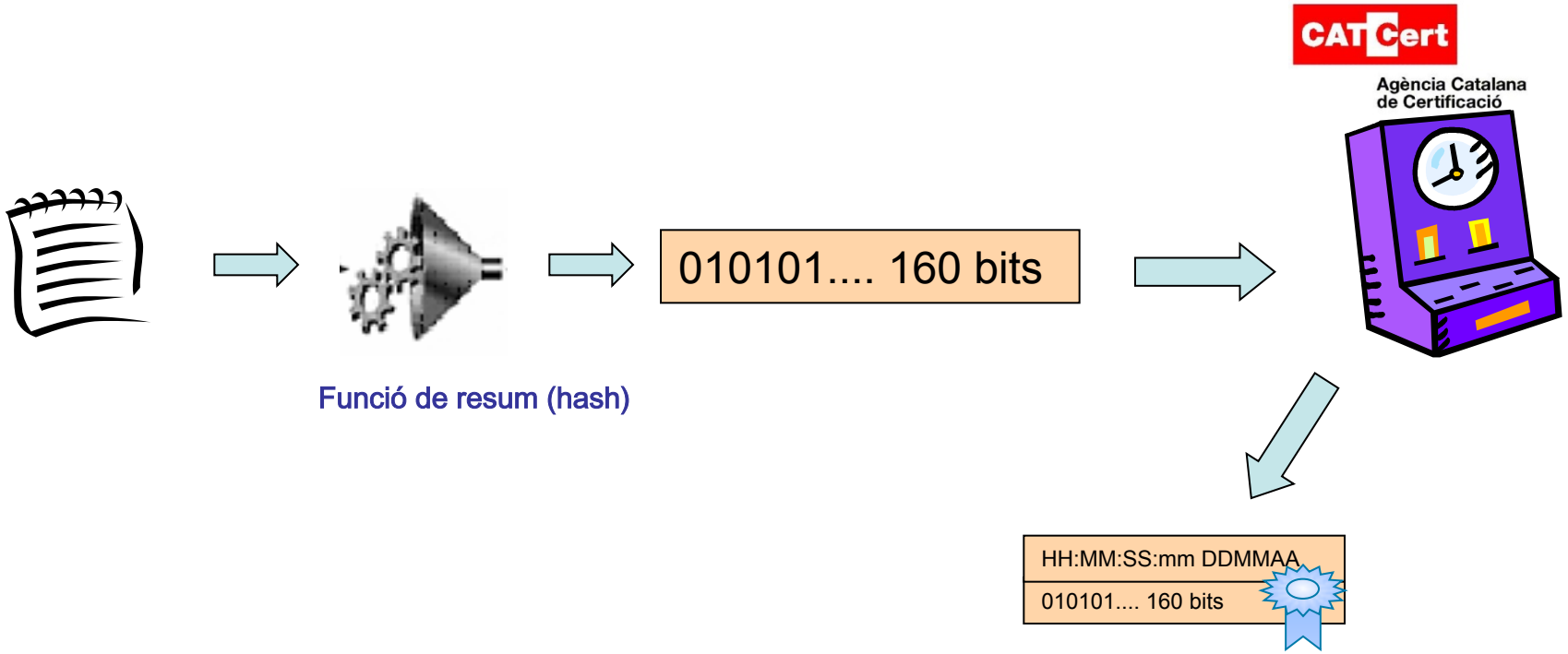


Firma electrónica y servicios de confianza – 7

Firma electrónica y servicios de confianza – 8



Firma electrónica y servicios de confianza – 9



Firma electrónica y servicios de confianza – 10

Prestadores de Servicios Criptográficos (PSC)				
Periodo	**Entidad**	**Algori**		
Presente - 2008	AC raíz	SH		
	AC subordinada y otras componentes de la PKI	SH		
A partir de 2008	AC raíz	SHA-512	ECDSA 512	A determinar
	AC subordinada y otras componentes de la PKI	SHA-384	ECDSA 384	

ENTIDADES FINALES			
Periodo	**Algoritmo y longitud mínima**		**Validez máxima certificado / clave privada**
	Hash	Firma	
Presente –2008	SHA-256	RSA 2048	2 años / 2 años
A partir de 2008	SHA-256	ECDSA 256	A determinar

Normas y estándares aplicables – 1

- La legislación no se desarrolla mediante reglamentos jurídicos, sino mediante la aprobación de normas técnicas producidas por ingenieros y otros actores.
- El European Telecommunication Standards Institute, bajo el Mandato 460 de la Comisión Europea, está trabajando en un Rationalised Framework for Electronic Signature Standardisation (SR 001 604 v1.1.1):
  - Creación y validación de firma electrónica.
  - Dispositivos de creación de firma y relacionados.
  - Suites criptográficas.
  - Proveedores de servicios de confianza que soportan firma electrónica.
  - Proveedores de servicios de aplicaciones de confianza.
  - Proveedores de estado de servicios de confianza (lista).

Normas y estándares aplicables – 2

- Rationalised Framework for Electronic Signature Standardisation (SR 001 604 v1.1.1). Tipos de documentos:
  - Guidance: This type of documents does not include any normative requirements but provides business driven guidance on addressing the eSignature (functional) area, on the selection of applicable standards and their options for a particular business implementation context and associated business requirements, on the implementation of a standard (or a series of standards), on the assessment of a business implementation against a standard (or a series of standards), etc.
  - Policy & Security Requirements: This type of document specifies policy and security requirements for services and systems, including protection profiles. This brings together use of other technical standards and the security, physical, procedural and personnel requirements for systems implementing those technical standards.

Normas y estándares aplicables – 3

- Rationalised Framework for Electronic Signature Standardisation (SR 001 604 v1.1.1). Tipos de documentos:
  - Technical Specifications: This type of document specifies technical requirements on systems. This includes but is not restricted to technical architectures (describing standardised elements for a system and their interrelationships), formats, protocols, algorithms, APIs, profiles of specific standards, etc.
  - Conformity Assessment: This type of document addresses requirements for assessing the conformity of a system claiming conformity to a specific set of technical specifications, policy or security requirements (including protection profiles when applicable). This primarily includes conformity assessment rules (e.g. common criteria evaluation of products or assessment of systems and services).

Normas y estándares aplicables – 4

- Rationalised Framework for Electronic Signature Standardisation (SR 001 604 v1.1.1). Tipos de documentos:
  - Testing Compliance & Interoperability: This type of document addresses requirements and specifications for setting-up interoperability tests or testing systems or for setting-up tests or testing systems that will provide automated checks of compliance of products, services or systems with specific set(s) of technical specifications.

Especialización y oportunidades profesionales

- El valor legal y, más concretamente, los efectos jurídicos de los servicios de confianza dependen de su correcto diseño y verificación del cumplimiento de los requisitos técnicos.
- Dos tipos de oportunidades profesionales:
  - Diseño, desarrollo, implementación.
  - Auditoría, evaluación de la conformidad.
- Dos potenciales tipos de clientes
  - Proveedores de servicios de confianza (pocos). Obligados por Ley a la auditoría.
  - Consumidores / usuarios de servicios de confianza (muchos). Auditoría voluntaria, pero imprescindible para la prueba electrónica.

La perspectiva del desarrollador

- Cumplimiento de los estándares internacionales y europeos (varias docenas…), aplicables a cada servicio.
- Desarrollo seguro, desarrollo seguro, desarrollo SEGURO (caso DigiNotar, Black Tulip report).
- Control adecuado de las vulnerabilidades, programas de parches, verificación de código, etc.
- Posibilidad de empleo de librerías certificadas de acuerdo con Common Criteria, o alternativamente, plantearse la certificación del código propio (aunque es muy caro).

La perspectiva del auditor – 1

- Creación y validación de firma electrónica:
  - EN 19 103 Conformity Assessment for Signature Creation and Validation Applications (& Procedures)
  - This document introduces the three aspects of assessment detailed in separate specifications:
  - a) Assessment of user environment against policy requirements: the conformity rules for assessing conformity of SCA or SVA against Policy Requirements.
  - b) Assessment of products and applications for electronic signature creation and validation against protection profiles.
  - c) Assessment of conformity to Advanced Electronic Signature formats and protocols.
  - d) Assessment of conformity of a specific machine processable signature policy to the business process policy requirements.

La perspectiva del auditor – 2

- Dispositivos de creación de firma y relacionados:
  - EN 19 203 Conformity Assessment of Secure Devices and Trustworthy systems
  - This document provides guidance on conformity assessment of Secure Creation Devices against the specifications EN 19 211 and guidance on conformity assessment for trustworthy systems against the specifications EN 19 221, EN 19 231, EN 19 241 and EN 19 251.The guidance is intended for use by designated bodies, assessors, evaluators and manufacturers.
  - Hoy se emplea, para dispositivos seguros de creación de firma, UNE-CWA 14169, y para sistemas fiables para la emisión y gestión de certificados, CEM CWA 14167, partes 1 a 4.

La perspectiva del auditor – 3

- Proveedores de servicios de confianza que soportan firma electrónica:
  - EN 19 403: General requirements and guidance for Conformity Assessment of TSPs Supporting Electronic Signatures
  - This document specifies general requirements for conformity assessment independent of the form of TSP and provides guidance for the supervision and assessment of a TSP supporting electronic signatures.
  - EN 19 413: Conformity Assessment for TSPs Issuing Certificates
  - This document specifies requirements and provides guidance for the supervision and assessment of a TSP issuing certificates.
  - EN 19 423 Conformity Assessment for TSPs providing Time-Stamping Services
  - This document specifies requirements and provides guidance for the supervision and assessment of a TSP providing time-stamping services.

La perspectiva del auditor – 4

- Proveedores de servicios de confianza que soportan firma electrónica:
  - EN 19 433 Conformity Assessment for TSPs providing Signature Generation Services
  - This document specifies requirements and provides guidance for the supervision and assessment of a TSP providing Signature Generation Services.
  - EN 19 443 Conformity Assessment for TSPs providing Signature Validation Services
  - This document specifies requirements and provides guidance for the supervision and assessment of a TSP providing Signature Validation Services.

La perspectiva del auditor – 5

- Proveedores de servicios de aplicaciones de confianza:
  - EN 19 513 Conformity Assessment of Registered Electronic Mail Service Providers
  - This document specifies requirements and provides guidance for the supervision and assessment of a Registered Electronic Mail Service Provider based on general requirements and guidance for conformity assessment specified in EN 19 403.
  - EN 19 523 Conformity Assessment of Data Preservation Service Providers
  - This document specifies requirements and provides guidance for the supervision and assessment of a DPSP based on general requirements and guidance for conformity assessment specified in EN 19 403.

La perspectiva del auditor – 6

- ¿En qué os puede ayudar ISACA?
  - Organización internacionalmente reconocida, entre otros dominios, en la práctica de auditoría.
  - Certificación en auditor de sistemas de información, CISA, apropiada para demostrar la competencia profesional a efectos de los estándares europeos.
  - Código ético y formación continuada, que son requisitos exigibles en todo caso.
  - ITAF, A Professional Practices Framework for IT Assurance (2008).
  - IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals (2010).
  - E-commerce and Public Key Infrastructure (PKI) Audit/Assurance Program (2012)

ISACA
Sistemas de información fiables y valiosos
Valencia Chapter

Gracias

Nacho Alamillo Domingo
investigacion@isacavalencia.org
nacho@astrea.cat

CISA Certified Information Systems Auditor An ISACA Certification
CISM Certified Information Security Manager An ISACA Certification
CGEIT Certified in the Governance of Enterprise IT An ISACA Certification
CRISC Certified in Risk and Information Systems Control An ISACA Certification