



Autoritat de Certificació de la Comunitat Valenciana

Seguridad en Autoridades de Certificación: *la Autoridad de Certificación de la Comunidad Valenciana*

ISACA Valencia Chapter #182

*Departamento de Organización de Empresas
Universidad Politécnica de Valencia*

Diciembre de 2004

Secretaría Autónoma de Telecomunicaciones y Sociedad de la Información
Conselleria de Infraestructuras y Transporte
Generalitat Valenciana



● Agenda

- Situación de las Autoridades de Certificación en España
- Requerimientos legales de seguridad
- Auditorías solicitadas y exigidas
- El caso de la ACCV
 - Estado de desarrollo
 - Situación respecto al marco legal
 - Objetivos de seguridad
 - Hitos alcanzados



- **Situación de las Autoridades de Certificación**
 - **Relación de Autoridades de Certificación o PSC**
 - **Ámbitos de los PSCs**
 - **Algunas cifras**
 - **Certificaciones de seguridad, sellos de calidad...**
 - **Condicionantes en el desarrollo**



● Situación de las Autoridades de Certificación

■ Relación de PSCs en España

1. **ANF-CA:** asociación nacional de fabricantes
2. **CERES (FNMT-RCM)**
3. **CAMERFIRMA:** Cámaras de Comercio
4. **FIRMAPROFESIONAL**
5. **GENERALITAT VALENCIANA**
6. **AC ABOGACIA**
7. **CICCP:** Colegio de Ingenieros de Caminos, Canales y Puertos
8. **ANCERT:** Agencia Notarial de Certificación
9. **BANESTO**
10. **IZENPE:** Diputaciones y Gobierno Vasco
11. **CATCERT:** Agencia Catalana de Certificación

Fuente: M° de Industria, Comercio y Turismo



- **Situación de las Autoridades de Certificación**
 - **Ámbitos de los PSCs (principales)**

	PUBLICO	SECTORIAL	PRIVADO
ANF-CA		✓	✓
CERES	✓	✓	✓
CAMERFIRMA		✓	✓
FIRMAPROFESIONAL		✓	
GENERALITAT VALENCIANA	✓		
AC ABOGACIA		✓	
CICCP		✓	
ANCERT		✓	
BANESTO			✓
IZENPE	✓	✓	
CATCERT	✓	✓	



● Situación de las Autoridades de Certificación

■ Algunas cifras

	Certs. emitidos	Puntos Registro Usuario	Convenios
ANF-CA	??	??	??
CERES	Más de 700.000	Más de 300	Más de 70
CAMERFIRMA	??	Cámaras de Comercio	N/A
FIRMAPROFESIONAL	??	Aprox. 16	Aprox. 16
GENERALITAT VALENCIANA	Aprox. 37.000	102 públicos + 42 restringidos = 144	41 Admón Local 18 (otras entidades)
AC ABOGACIA	??	??	??
CICCP	??	??	??
ANCERT	??	??	??
BANESTO	??	??	??
IZENPE	??	6	N/A
CATCERT	??	5	N/A



● Situación de las Autoridades de Certificación

usuarios FNMT

Comunidad Autónoma	Usuarios activos a 1 de Julio de 2004	% sobre el total de usuarios	Población a 1 de Enero de 2003	% de penetración en la población
Madrid (Comunidad de)	135.643	23,50%	5.718.942	2,372%
Andalucía	95.817	16,60%	7.606.848	1,260%
Cataluña	94.162	16,32%	6.704.146	1,405%
Comunidad Valenciana	53.929	9,34%	4.470.885	1,206%
Castilla y León	33.797	5,86%	2.487.646	1,359%
Galicia	27.267	4,72%	2.751.094	0,991%
Aragón	20.690	3,59%	1.230.090	1,682%
Canarias	19.626	3,40%	1.894.868	1,036%
Castilla-La Mancha	16.727	2,90%	1.815.781	0,921%
Asturias (Principado de)	16.200	2,81%	1.075.381	1,506%
Murcia (Región de)	13.917	2,41%	1.269.230	1,096%
Balears (Illes)	11.273	1,95%	947.361	1,190%
País Vasco	8.514	1,48%	2.112.204	0,403%
Extremadura	8.040	1,39%	1.073.904	0,749%
Cantabria	6.898	1,20%	549.690	1,255%
Navarra (Comunidad Foral de)	6.071	1,05%	578.210	1,050%
Rioia (La)	4.854	0,84%	287.390	1,689%
Melilla	1.915	0,33%	68.463	2,797%
Ceuta	1.779	0,31%	74.931	2,374%
Residentes en el Extranjero	66	0,01%		
TOTAL	577.119	100,00%		



- **Situación de las Autoridades de Certificación**
 - **Certificaciones de seguridad, sellos de calidad...**

	Cert. Seguridad	Cert. Conformidad	Sellos calidad y otros
ANF-CA	NO	Orden HAC/1181/2003	NO
CERES	NO	NO	ISO 9001:2000 Sello calidad Internet (IQUA)
CAMERFIRMA	Webtrust	R.D. 14/1999 Orden HAC/1181/2003	NO
FIRMAPROFESIONAL	Webtrust	Ley 59/2003 Orden HAC/1181/2003	NO
GENERALITAT VALENCIANA	NO (en desarrollo WT)	Orden HAC/1181/2003 LOPD	NO
AC ABOGACIA	Webtrust	Orden HAC/1181/2003	NO
CICCP	??	??	??
ANCERT	??	Orden HAC/1181/2003	??
BANESTO	NO	Orden HAC/1181/2003	NO
IZENPE	NO	Orden HAC/1181/2003	NO
CATCERT	NO	Orden HAC/1181/2003	NO



● Situación de las Autoridades de Certificación

■ Condicionantes en el desarrollo

- Posibilidad de utilización para acceso a aplicaciones y servicios públicos telemáticos (AEAT, TGSS, Generalitat en Red...)
- **Reconocimiento** por parte de productos estándar (navegadores web, clientes de correo-e...)
- Soporte del certificado (criptográfico o software)
- Diversidad de formatos y perfiles de certificados

**El valor del certificado es proporcional
al valor de los servicios para los que es necesario**



● **Requerimientos legales de seguridad**

■ **Regulación principal**

- **COMUNITARIA:** directiva europea 1999/93/CE, de 13 de diciembre
- **ESPAÑOLA:** ley 59/2003, de 19 de diciembre, de firma electrónica (tras el derogado R.D-I 14/1999)
- **AUTONÓMICA VALENCIANA:** decreto 87/2002, de 30 de mayo, del Gobierno Valenciano (sólo ámbito GV y entidades con las que convenia)



● Requerimientos legales de seguridad

■ Resumen de exigencias de seguridad:

- Protección de datos de carácter personal (**LOPD**)
- Disponer de una **Declaración de Prácticas de Certificación**, con carácter de *Documento de Seguridad*
- Disponer de **fiabilidad necesaria** para prestar servicios de certificación
- Emplear personal **cualificado**
- Utilizar productos y sistemas **fiables**
- **Tomar medidas** contra la falsificación de certificados



● Requerimientos legales de seguridad

■ Exigencias de seguridad (ii):

- CONCLUSIONES:

- Poco detalle y sin desarrollo reglamentario de la Ley. Corrientes legislativas/normativas favorables a la autorregulación del *mercado* y la industria relacionada
- Conveniencia de determinar normativa técnica y de seguridad que cumplir. Dependiente de evolución de mercado e industria y la regulación técnica que se asuma
- Normativa técnica y de seguridad debe ser homogénea a lo largo de la UE



● Requerimientos legales de seguridad

■ Exigencias de seguridad (iii):

- Necesidad de iniciar la generación de normativa técnica y de seguridad que desarrolla la directiva europea de firma electrónica (1999/93/CE)
- **EESSI**: European Electronic Signature Standardization Initiative, creado por el ICTSB (Information & Communications Technologies Standards Board) para el desarrollo de la directiva 1999/93/CE
- Actividades de EESSI a cargo de **CEN** (Comité Europeo de Normalización) y **ETSI** (European Telecommunications Standard Institute)



● **Requerimientos legales de seguridad**

■ **Exigencias de seguridad (iv):**

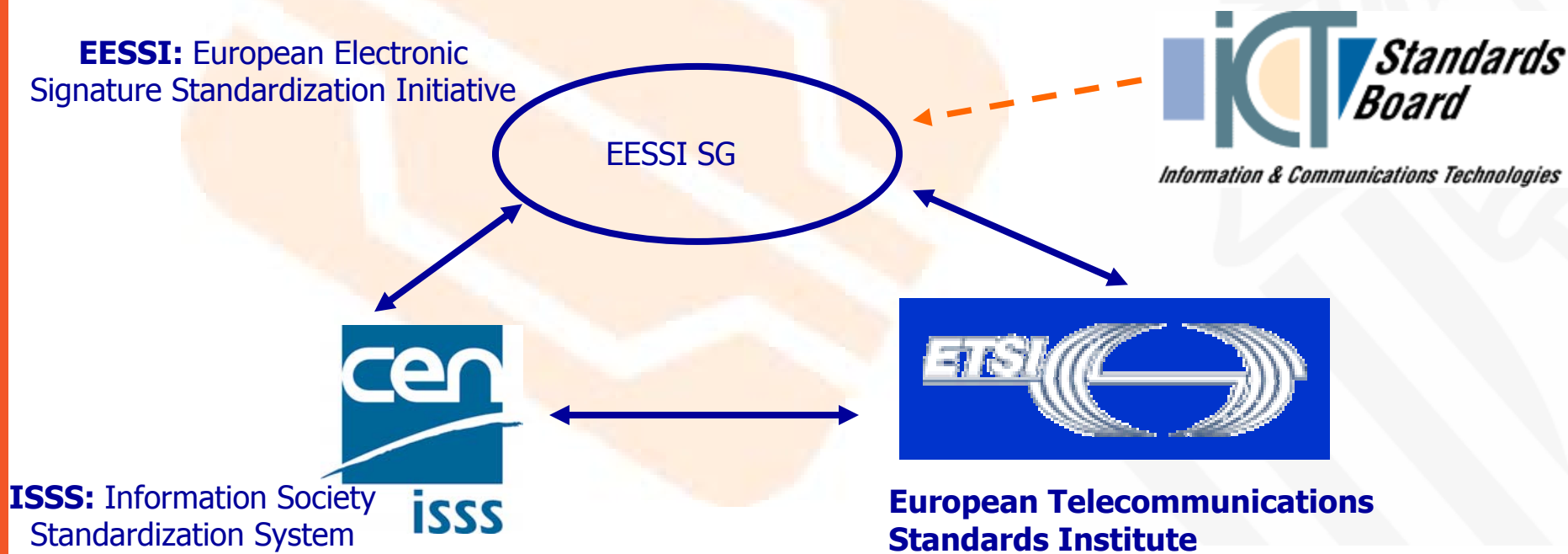
- Resultado de actividades de EESSI (CEN y ETSI) no son normas de cumplimiento obligatorio: son especificaciones técnicas
- Las especificaciones técnicas desarrollan los requerimientos de la directiva 1999/93/CE, establecen unos mínimos a cumplir y un marco de comparación de los servicios y su forma de prestación
- Pueden constituir los elementos para el desarrollo de sistemas voluntarios de acreditación comúnmente aceptados



● Requerimientos legales de seguridad

■ Exigencias de seguridad (v):

- Los organismos de estandarización europeos proporcionan un marco abierto y orientado al mercado para la implantación de la directiva de firma-e





● Auditorías solicitadas y exigidas

- ¿Qué sucede ante la NO exigencia legal de auditorías o certificaciones concretas?
- Ante un mercado de servicios de certificación de muy lento desarrollo y de muy lenta recuperación de inversión
- Despliegue de certificados condicionado por aplicaciones y servicios telemáticos de Administraciones Públicas (AEAT, TGSS, GV en RED...)
- Ante el hecho de que la confianza en los certificados expedidos por un PSC esté vinculada a inclusión de los certificados de las CAs en los navegadores web o clientes de correo electrónico más populares

PSCs se someten a las auditorías mínimas exigidas por las AAPP prestadoras de servicios telemáticos o por los fabricantes de los navegadores, etc...

**autorregulación
del mercado**



● Auditorías solicitadas y exigidas

- **Para aceptación por parte de AEAT: informe sobre cumplimiento** de los requisitos de la Orden HAC/1181/2003, emitido por un tercero independiente con solvencia técnica en el análisis y evaluación de la prestación de serv. de certificación
- **Para aceptación por parte de otras Administraciones: NO formalizado:** condiciones al vuelo, réplica de condiciones de la AEAT, condiciones exclusivamente de técnicas... Parece que la vía que seguirá el M^o de Industria en la evaluación y control de PSCs se basará en los criterios establecidos por ASIMELEC junto con ASIA (Madrid ISACA Chapter) y algunos PSCs



● Auditorías solicitadas y exigidas

- **Para inclusión de certificados en Windows (para MS Internet Explorer, MS Outlook, MS Outlook Express, etc.): desde aprox. año 2001, superar auditoría WebTrust para CAs**
- **Para inclusión de certificados en Mozilla Foundation (Mozilla, Firefox, Thunderbird, etc.): desde aprox. año 2003, superar auditoría WebTrust para CAs**



● Auditorías solicitadas y exigidas



■ Auditoría y Certificación ASIMELEC/ASIA

- Certificación sobre los servicios de emisión de certificados digitales de los PSCs
- Dos tipos de certificados:
 - certificados para la firma electrónica
 - certificados de sellado de tiempo
- En ambos casos hay tres niveles de certificados:
 - certificado normalizado / sellado de tiempo básico
 - certificado reconocido / sellado de tiempo normalizado
 - certificado excelente / sellado de tiempo excelente



● Auditorías solicitadas y exigidas



■ Auditoría y Certificación ASIMELEC/ASIA (ii)

● Firma electrónica

- Normalizado: cumplimiento de **ETSI TS 102 042** (Policy requirements for certification authorities issuing public key certificates)
- Reconocido: (satisface requisitos de la Ley 59/2003) cumplimiento de **ETSI 101 456** (Policy requirements for certification authorities issuing qualified certificates) y **CWA 14167-1** (Security requirements for Trustworthy Systems Managing Certificates for electronic signatures)
- Excelente: requisitos del certificado reconocido y, además, cumplimiento de **ETSI 101 862** (Qualified certificate profile)
 - plazo de publicación de CRLs de 3 horas o inferior
 - servicios de call-center 24x7
 - sistema de gestión de la calidad **ISO 9000**
 - sistema de gestión de la seguridad conforme **ISO 17799**



● Auditorías solicitadas y exigidas



■ Auditoría y Certificación ASIMELEC/ASIA (iii)

- Firma electrónica: verificación del cumplimiento de los requisitos establecidos conforme a las normas
 - **CWA 14172-1:** EESSI Conformity Assessment Guidance – Part 1: General introduction
 - **CWA 14172-2:** EESSI Conformity Assessment Guidance – Part 2: Certification Authority services and processes
 - **CWA 14172-3:** EESSI Conformity Assessment Guidance – Part 3: Trustworthy systems managing certificates for electronic signatures



● Auditorías solicitadas y exigidas



■ Auditoría y Certificación ASIMELEC/ASIA (iv)

• Sellado de tiempo

- Básico: cumplimiento de apdos. 7.3.2 y 7.2.2 de **ETSI TS 102 023** (Policy requirements for time-stamping authorities)
- Normalizado: cumplimiento de **ETSI 102 023** (Policy requirements for time-stamping authorities)
- Excelente: cumplimiento de **ETSI 102 023** (Policy requirements for time-stamping authorities), **ETSI 101 861** (Time stamping profile)
 - precisión superior al segundo
 - servicios de call-center 24x7
 - sistema de gestión de la calidad **ISO 9000**
 - sistema de gestión de la seguridad conforme **ISO 17799**.



- Auditorías solicitadas y exigidas



- Auditoría y Certificación ASIMELEC/ASIA (iii)

- Sellado de tiempo: verificación del cumplimiento de los requisitos establecidos conforme a la norma
 - **CWA 14172-8**: EESSI Conformity Assessment Guidance – Part 8: Timestamping Authority services and processes



● Auditorías solicitadas y exigidas

■ Principales requerimientos de ETSI 101 456: *Policy requirements for certification authorities issuing qualified certificates*

- 7.1 Declaración de Prácticas de Certificación
- 7.2 PKI – Gestión del ciclo de vida de las claves
- 7.3 PKI – Gestión del ciclo de vida de los certificados
- 7.4 Gestión y Operación de la CA
- 7.5 Organización



● Auditorías solicitadas y exigidas

■ Principales requerimientos de ETSI 101 456 (ii)

7 Requirements on CA practice

7.1 Certification practice statement

No indica norma a seguir ni estructura. Es recomendable seguir otras normas para la redacción de la CPS (como por ejemplo RFC 3647)

7.2 Public key infrastructure - Key management life cycle

- 7.2.1 Certification authority key generation
- 7.2.2 Certification authority key storage, backup and recovery
- 7.2.3 Certification authority public key distribution
- 7.2.4 Key escrow
- 7.2.5 Certification authority key usage
- 7.2.6 End of CA key life cycle
- 7.2.7 Life cycle management of cryptographic hardware used to sign certificates
- 7.2.8 CA provided subject key management services
- 7.2.9 Secure-signature-creation device preparation

7.3 Public key infrastructure - Certificate Management life cycle

- 7.3.1 Subject registration
- 7.3.2 Certificate renewal, rekey and update
- 7.3.3 Certificate generation
- 7.3.4 Dissemination of Terms and Conditions
- 7.3.5 Certificate dissemination
- 7.3.6 Certificate revocation and suspension

7.4 CA management and operation

- 7.4.1 Security management
- 7.4.2 Asset classification and management
- 7.4.3 Personnel security
- 7.4.4 Physical and environmental security
- 7.4.5 Operations management
- 7.4.6 System Access Management
- 7.4.7 Trustworthy Systems Deployment and Maintenance
- 7.4.8 Business continuity management and incident handling
- 7.4.9 CA termination
- 7.4.10 Compliance with Legal Requirements
- 7.4.11 Recording of Information Concerning Qualified Certificates

7.5 Organizational



- **Auditorías solicitadas y exigidas**
 - **Principales requerimientos de CWA 14167-1: *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements***
 - 5.1 Requerimientos Generales de Seguridad
 - 5.2 Requerimientos de seguridad de los servicios básicos (obligatorios)
 - 5.3 Requerimientos de seguridad de los servicios opcionales



● Auditorías solicitadas y exigidas

■ Principales requerimientos de CWA 14167-1 (ii)

5 Security Requirements

5.1 General Security Requirements

- 5.1.1 Management
- 5.1.2 Systems & Operations
- 5.1.3 Identification & Authentication
- 5.1.4 System Access Control
- 5.1.5 Key Management
- 5.1.6 Accounting & Auditing
- 5.1.7 Archiving
- 5.1.8 Backup & Recovery

5.2 Core Services Security Requirements

- 5.2.1 General
- 5.2.2 Registration Service
- 5.2.3 Certificate Generation Service
- 5.2.4 Dissemination Service
- 5.2.5 Certificate Revocation Management Service
- 5.2.6 Certificate Revocation Status Service

5.3 Supplementary Services Security Requirements

- 5.3.1 Time-Stamping Service
- 5.3.2 Subject Device Provision Service



- **Auditorías solicitadas y exigidas**

- **Inclusión de certificados de PSC en productos Windows (navegador web, clientes de correo-e, etc.)**
- **Inclusión de certificados en productos de Mozilla Foundation (navegadores web, clientes de correo-e, etc.)**



WebTrust for Certification Authorities



● Auditorías solicitadas y exigidas

■ WebTrust

- Certificaciones avaladas por
 - AICPA: American Institute of Certified Public Accountants
 - CICA: Canadian Institute of Chartered Accountants
- Prevé 5 tipos de sellos:
 - **Sello Genérico.** Para combinación de, seguridad, prácticas de negocio e integridad de las transacciones, confidencialidad y disponibilidad.
 - **Sello de Privacidad.** Expedido para privacidad on-line.
 - **Sello Protección del Consumidor.** Para entidades que cumplan los Principios y Criterios de Privacidad y Prácticas de Negocio e Integridad de las Transacciones.
 - **Sello para Autoridades de Certificación.** Expedido para CA que cumplen criterios específicos de Certification Authorities.
 - **Sello para Proveedores de Servicio.** Se expedirá a entidades que cumplan con los módulos requeridos. (Actualmente no finalizados, en fase de consultas y comentarios)



● Auditorías solicitadas y exigidas

■ WebTrust para CAs: criterios basados en ANSI X9.79

- Principle 1: CA Business Practices Disclosure (CPS)
- Principle 2: Service Integrity
- Principle 3: CA Environmental Controls

Sigue estándar ANSI X9.79 *PKI Practices and Policy Framework*



● Auditorías solicitadas y exigidas

■ WebTrust para CAs – P2: Service Integrity

- Key life cycle management controls
 - CA key generation
 - CA key storage, backup and recovery
 - CA public key distribution
 - CA key escrow (optional)
 - CA key usage
 - CA key destruction
 - CA key archival
 - CA cryptographic hardware life cycle management
 - CA-provided subscriber key management services (optional)



● Auditorías solicitadas y exigidas

■ WebTrust para CAs – P2: Service Integrity (ii)

- Certificate life cycle management controls
 - Subscriber registration
 - Certificate renewal (optional)
 - Certificate rekey
 - Certificate issuance
 - Certificate distribution
 - Certificate revocation
 - Certificate suspension (optional)
 - Certificate status information processing
 - Integrated Circuit Card (ICC) life cycle management (optional)



● Auditorías solicitadas y exigidas

■ **WebTrust para CAs – P3: CA Environmental Controls**

- Certification Practice Statement and Certificate Policy Management
- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- Systems Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Event journaling



● El caso de la ACCV

■ Estado de desarrollo

- ¿Qué es la ACCV?
- ¿Qué servicios presta?
- ¿A quién presta los servicios?
- ¿Qué se puede hacer con el certificado de la ACCV?
- Algunas cifras

■ Situación respecto al marco legal

■ Objetivos de seguridad

■ Hitos alcanzados



● El caso de la ACCV: estado de desarrollo

■ ¿Qué es la ACCV?

- ACCV es la entidad que expide y gestiona los certificados digitales y claves, es decir, la que certifica el vínculo entre una clave y una entidad (persona, servidor informático, código, aplicación...)
- Uno de los pilares para el desarrollo de la Sociedad de la Información en la Comunidad Valenciana



● El caso de la ACCV: estado de desarrollo

■ ¿Qué servicios presta?

Servicios básicos tal y como describe el CEN
(Comité Europeo de Normalización)
Workshop Agreement *CWA 14167-1*

1. **Servicios de Registro** para verificar la identidad de los usuarios, cara a cara
2. **Servicio de Generación de certificados**
 - para personas físicas
 - para servidores web seguros
 - para firma de código
 - ...
3. **Servicios de información** para publicar:
 - certificados (usuarios, entidades y CA's)
 - listas de certificados revocados (CRLs)...



● El caso de la ACCV: estado de desarrollo

■ ¿Qué servicios presta? (ii)

Servicios básicos tal y como describe el CEN
(Comité Europeo de Normalización)
Workshop Agreement *CWA 14167-1*

4. Servicios de Gestión de Revocación para permitir la invalidación de los certificados

5. Servicio de Validación para proporcionar información actualizada sobre el estado de los certificados:

- Generación de Listas de Certificados Revocados (CRL)
- Online Certificate Status Protocol (OCSP)
- Web services para mayor flexibilidad y servicios añadidos (comprobación de la integridad de la firma)

6. Servicio de Provisión de Dispositivos para facilitar al usuario la adquisición de éstos (tarjetas criptográficas actualmente)



● El caso de la ACCV: estado de desarrollo

- ¿Qué servicios presta? (iii)

Servicios adicionales según el CEN
(Comité Europeo de Normalización)
Workshop Agreement *CWA 14167-1*

7. Servicios de Sellado de Tiempo para garantizar la existencia de un documento o firma antes de un determinado instante. Básico para Registro Telemático y para la verificación de la firma a largo plazo
8. Servicio de Archivado de Claves de cifrado (exclusivamente)



● El caso de la ACCV: estado de desarrollo

■ ¿Qué servicios presta? (iv)

Otros servicios sin catalogación CEN

9. Soporte al análisis y desarrollo de aplicaciones

- consultoría de proyectos con uso de certificación
- librerías criptográficas de alto nivel
- enlace entre equipos de desarrollo

10. Soporte a usuarios finales (ETSI sí que cita la información a usuarios)

- Call Center
- Guías técnicas y de procedimiento
- Generación de FAQs

11. Servicios de Formación, también sobre plataforma de eLearning:

- usuarios finales (empleados públicos, ciudadanos ...)
- desarrolladores y responsables de proyectos
- operadores de Call Center y de Punto de Registro



● El caso de la ACCV: estado de desarrollo

■ ¿A quién presta los servicios?

- Generalitat Valenciana
- Organismos y entes autónomos dependientes
- Administración Local valenciana
- Ciudadanos y Profesionales en sus relaciones con las Administraciones Públicas

- Servicios de la Administración General del Estado
 - Agencia Estatal de Administración Tributaria (AEAT)
 - Tesorería General de la Seguridad Social
 - Mº de Justicia
 - DG del Catastro





● El caso de la ACCV: estado de desarrollo

■ ¿Qué se puede hacer con el certificado de la ACCV?

- Generalitat en Red  **Generalitat en RED** ver tramita.gva.es
- Infoville 21  **infoville 21**
 - autenticación ante el Portal basada en certificado
 - integración de sistema de autenticación
- SERVEF (servicio valenciano de empleo y formación) 
 - Servicios Interactivos, para demandantes de empleo
 - Solicitud de Cursos
 - Extranet de SERVEF (Centros Asociados, Oficinas, etc.)



● El caso de la ACCV: estado de desarrollo

■ ¿Qué se puede hacer con el certificado de la ACCV?

- eSMAC: arbitraje y conciliación laboral (www.gva.es)
- Arbitraje Virtual de Consumo (www.gva.es)
- ADCR: gestión y control de residuos industriales
- Abucasis-II: sistemas de información sanitarios
 - GAIA, para gestión de receta sanitaria
 - control y gestión de boletines analíticos
 - sistemas de control de acceso y firma de historias clínicas
- eFormación (eformacion.gva.es)
 - autenticación en plataforma
 - expedición de certificados de aprovechamiento
- Remisión de documentos al DOGV (proy. ENDOGV)



● El caso de la ACCV: estado de desarrollo

■ ¿Qué se puede hacer con el certificado de la ACCV?

- Catarroja Ajuntament Virtual
- Ayuntamiento de Valencia
- Ayuntamiento de Alicante
- SUMA Gestión Tributaria
- Oficina Virtual de la Agencia Tributaria
- Tesorería General de la Seguridad Social
- Registro General Telemático del IMPIVA
- Oficina Virtual del Catastro (Mº Economía y Hacienda)
- Acceso a LexNet (Mº Justicia) ...





- **El caso de la ACCV: situación respecto al marco legal**
 - **Cumplimiento de las exigencias de la Ley 59/2003, de 19 de diciembre**
 - **Cumplimiento de las exigencias del Decreto 87/2002, de 30 de mayo, del Gobierno Valenciano**
 - **Pendiente de publicación en página del Mº de Industria, Comercio y Turismo: desacuerdo por régimen de responsabilidad patrimonial de la Administración Pública**
 - **La determinación efectiva del cumplimiento de la Ley se hará tras la evaluación y control del Mº de Industria**



● El caso de la ACCV: objetivos de seguridad

- **Cumplimiento de "certificación ASIMELEC", es decir:**
 - certificados de firma electrónica
 - ETSI 101 456
 - CWA 14167-1
 - ETSI 102 862 (sólo perfil)
 - certificados de sello de tiempo
 - ETSI 102 023
 - ETSI 101 861 (sólo perfil)

antes de abril '05



- **El caso de la ACCV: objetivos de seguridad**
 - **Finalización de auditoría WebTrust para CAs**
antes de abril '05
 - **Finalización del establecimiento de objetivos de control ISO 17799**
 - **Inicio implantación Sistema de Gestión de la Seguridad, certificable conforme a norma UNE 71502**
mayo / junio '05



- **El caso de la ACCV: hitos alcanzados**
 - **Proyecto de adecuación a LOPD y reglamento**
 - **Cubiertos requisitos WebTrust para CA a excepción de plan de continuidad del negocio, que está en desarrollo**
 - **Análisis diferencial contra ISO 17799**
 - **Análisis diferencial contra ETSI 101 456**
 - **Análisis diferencial contra CWA 14167-1**
 - **Análisis diferencial contra UNE 71502:2004**



● El caso de la ACCV: hitos alcanzados

- **Concienciación de personal de ACCV en materias de seguridad y protección de datos**
- **Concienciación y formación del personal en aspectos de formalización y gestión de los servicios**



● Referencias

- Autoritat de Certificació de la Comunitat Valenciana: <http://www.pki.gva.es>
- ETSI: <http://www.etsi.org>
- CEN: <http://www.cenorm.be>
- CEN/ISSS: <http://www.cenorm.be/issc>
- EESSI: http://www.ictsb.org/EESSI_home.htm
- CERES: <http://www.cert.fnmt.es>
- CatCERT: <http://www.catcert.net>
- Izenpe: <http://www.izenpe.net>
- Ministerio Industria, Comercio y Turismo: <http://www.min.es>
- Camerfirma: <http://www.camerfirma.com>
- ASIMELEC: <http://www.asimelec.es>
- WebTrust España: <http://www.webtrust.es/index.htm>
- AICPA: <http://www.aicpa.org>
- CICA: <http://www.cica.ca>



**Autoritat de Certificació
de la Comunitat Valenciana**



www.pki.gva.es

firma@gva.es

Tel. soporte: 902 482 481

Joaquín Galeano, CISA

galeano_joa@gva.es

Autoritat de Certificació de la Comunitat Valenciana

D.G. de Telecomunicaciones e Investigación

Secretaría Autónoma de Telecomunicaciones y Sociedad de la Información

Conselleria de Infraestructuras y Transporte