IX JORNADAS STIC CCN-CERT

DETECCIÓN E INTERCAMBIO, FACTORES CLAVE

Madrid, 10 y 11 de diciembre 2015

Exfiltración por canal lateral. ¿Son las certificaciones la solución?

CENTRO CRIPTOLÓGICO NACIONAL

ESQUEMA DE EVALUACIÓN Y CERTIFICACIÓN DE LA SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN

- Luis Hernández Encinas
- Agustín Martín Muñoz

- Instituto de Tecnologías Físicas y de la Información “Leonardo Torres Quevedo”
- Consejo Superior de Investigaciones Científicas
  - {luis, agustin}@iec.csic.es

Índice

1. Seguridad teórica/Seguridad matemática

1.1. ¿Es la seguridad teórica/matemática una garantía suficiente?

- **Principio de Kerckhoff** (1883): “La seguridad de un criptosistema no debe depender de mantener secreto el algoritmo de cifrado empleado. La seguridad depende sólo de mantener secreta la clave”.
- **Hipótesis de partida**: el atacante lo conoce casi todo: criptosistema, texto cifrado, algoritmos, técnicas computacionales, etc. El atacante sólo desconoce el texto en claro y la clave utilizada.
- Necesidad de utilizar problemas matemáticos “**computacionalmente difíciles**”: factorización, logaritmo discreto, (primalidad).

1.2. Factorización

Calcular la descomposición de un número dado como producto de números primos elevados a potencias: $3630 = 2 \cdot 3 \cdot 5 \cdot 11^2$.

RSA768 =

1230186684 5301177551 3049495838 4962720772 8535695953 3479219732
2452151726 4005072636 5751874520 2199786469 3899564749 4277406384
5925192557 3263034537 3154826850 7917026122 1429134616 7042921431
1602221240 4792747377 9408066535 1419597459 8569021434 13

=

3347807169 8956898786 0441698482 1269081770 4794983713 7685689124
3138898288 3793878002 2876147116 5253174308 7737814467 999489

x

3674604366 6799590428 2446337996 2795263227 9158164343 0876426760
3228381573 9666511279 2333734171 4339681027 0092798736 308917.

1.3. Desafío

RSA2048 =

2519590847 5657893494 0271832400 4839857142 9282126204
0320277771 3783604366 2020707595 5562640185 2588078440
6918290641 2495150821 8929855914 9176184502 8084891200
7284499268 7392807287 7767359714 1834727026 1896375014
9718246911 6507761337 9859095700 0973304597 4880842840
1797429100 6424586918 1719511874 6121515172 6546322822
1686998754 9182422433 6372590851 4186546204 3576798423
3871847744 4792073993 4236584823 8242811981 6381501067
4810451660 3773060562 0161967625 6133844143 6038339044
1495263443 2190114657 5444541784 2402092461 6515723350
7787077498 1712577246 7962926386 3563732899 1215483143
8167899885 0404453640 2352738195 1378636564 3912120103
9712282212 0720357.

1.4. Seguridad equivalente según tamaño de claves (en bits)

Nivel de seguridad	RSA y DHKA	Curvas elípticas
80	1.024	160-223
112	2.048	224-255
128	3.072	256-283
192	8.192	384-511
256	15.360	512-571

- D. Hankerson, A. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer, NY, 2004.
- NIST, *Digital Signature Standard* (DSS), FIPS 186-3, 2009.

1.5. Criptoanálisis actual

- **Hasta 1996**: la seguridad se basaba en la fortaleza matemática de los algoritmos criptográficos.

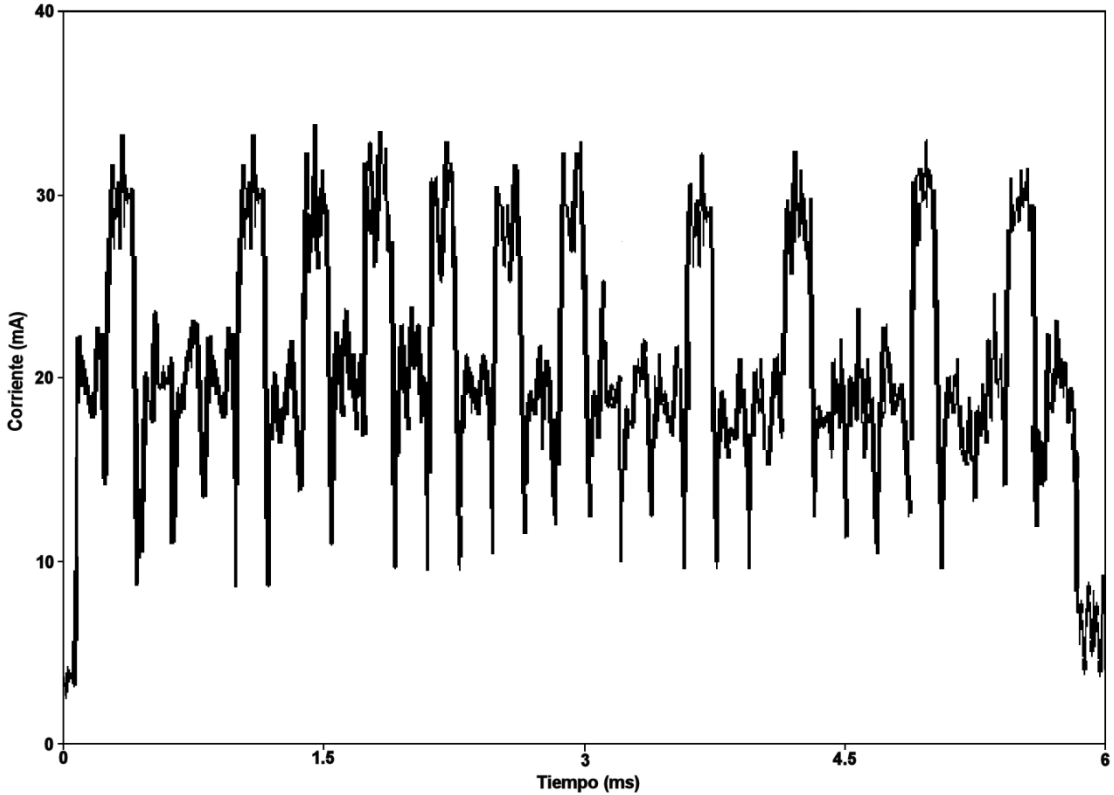
- **Desde 1996:** la seguridad se basa, además, en la correcta implementación de los algoritmos y en la **no vulnerabilidad de los dispositivos físicos** donde están implementados:
  - Ataque por inducción de fallos contra el RSA-CRT (Boneh, Demillo y Lipton, Eurocrypt'1997).
  - Ataque por análisis temporal contra RSA, Diffie-Hellman, DSS y otros (Kocher).

2. Seguridad de los dispositivos físicos criptográficos

Exfiltración: Ataques por canales laterales e inducción de fallos

- Vías a través de las que se puede exfiltrar información:
  - Modificaciones en el consumo de potencia.
  - Tiempo que dura una computación.
  - Niveles de temperatura que alcanza el dispositivo mientras está calculando.
  - Emisión de radiación electromagnética.
  - Diferentes niveles de ruido (sonido).
  - Inducción de fallos.

2.1. Análisis Simple de Potencia (*Simple Power Analysis, SPA*)



Consumo de potencia durante la ejecución del algoritmo RSA en una tarjeta sin contramedidas

Exponenciación modular en RSA (*square & multiply from left to right*)

- Operación a realizar: $y = x^k \pmod n$
- Clave: $k = (k_r, k_{r-1}, ..., k_1, k_0)_2$

- Algoritmo:

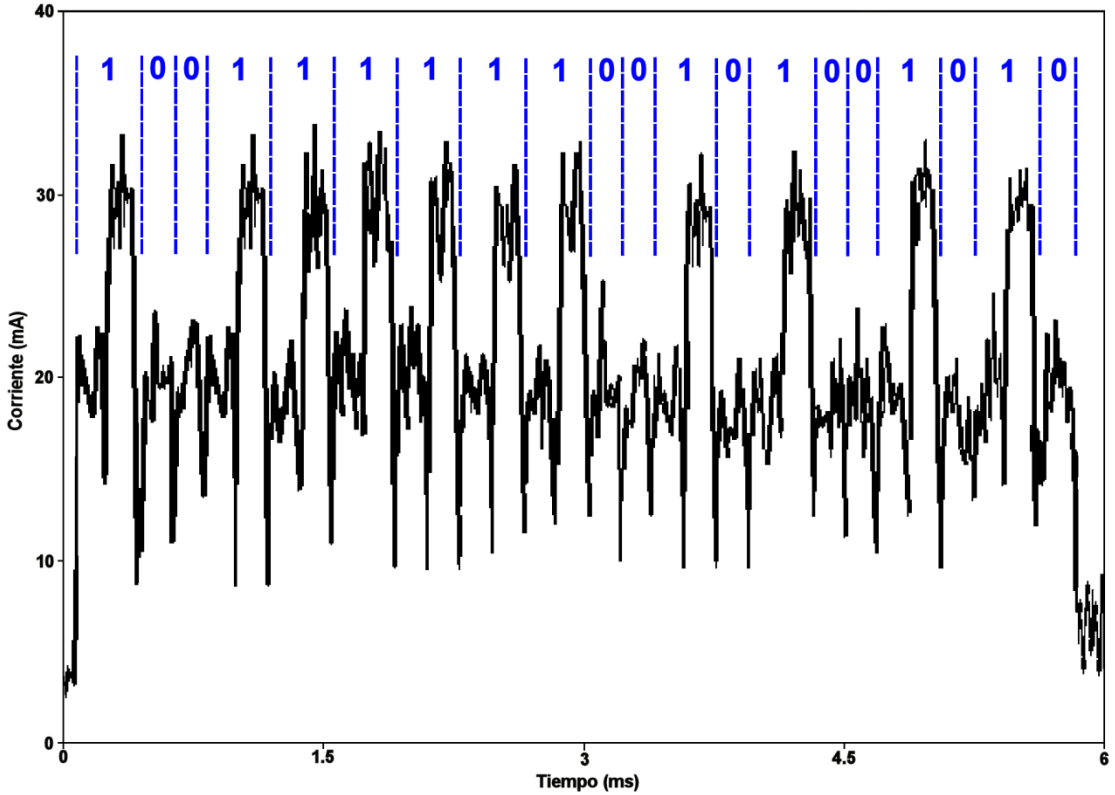
1. $y = x$
2. for $i = (r - 1)$ to 0 do
   1) $y = y^2 \pmod n$
   2) if $k_i = 1$ then $y = y \cdot x \pmod n$
3. return (y)

$$k = 23 = (10111)_2$$

$$y = x$$
$$i = 3, y = x^2$$
$$i = 2, y = (x^2)^2 x$$
$$i = 1, y = ((x^2)^2 x)^2 x$$
$$i = 0, y = (((x^2)^2 x)^2 x)^2 x$$

$$a^{23} = (((a^2)^2 a)^2 a)^2 a$$

Consumo de potencia en un cifrado RSA



La clave es:

$$k = (10011111100101001010)_2 = 653642$$

2.2. Análisis Diferencial de Potencia (*Differential Power Analysis, DPA*)

Platinum Sponsor

Rambus CRYPTOGRAPHY RESEARCH

Gold Sponsors

SERMA TECHNOLOGIES Serma Group

THALES

Région BRETAGNE

PÔLE D'EXCELLENCE CYBER

Organizers

CRYPTO EXPERTS

UPMC SORBONNE UNIVERSITÉS

CHES 2015

INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH

COSADE '2015

Sponsors

BOSCH Invented for life

TEXAS INSTRUMENTS

NXP

riscure

AIRBUS DEFENCE & SPACE

UL

orange

oberthur TECHNOLOGIES THE M COMPANY

Microsemi

Scytl Innovating Democracy

INVIA

technicolor

cea

infineon

ChaoLogix

SECURE IC

gemalto security to be free

Microsoft

GOLDEN SPONSORS

BOSCH Invented for life

infineon

riscure

SECURE IC THE TRUSTED COMPUTING COMPANY

TÜVIT TÜV NORD GROUP

SILVER SPONSORS

CRYPTOGRAPHY RESEARCH a division of Rambus

oberthur TECHNOLOGIES THE M COMPANY

NXP

2.3. Análisis Temporal (*Timming Analysis*)

Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems

Paul C. Kocher

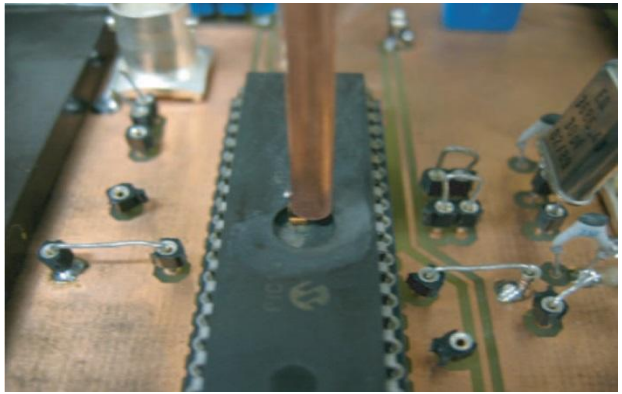
Cryptography Research, Inc.
607 Market Street, 5th Floor, San Francisco, CA 94105, USA.
E-mail: paul@cryptography.com.

1996

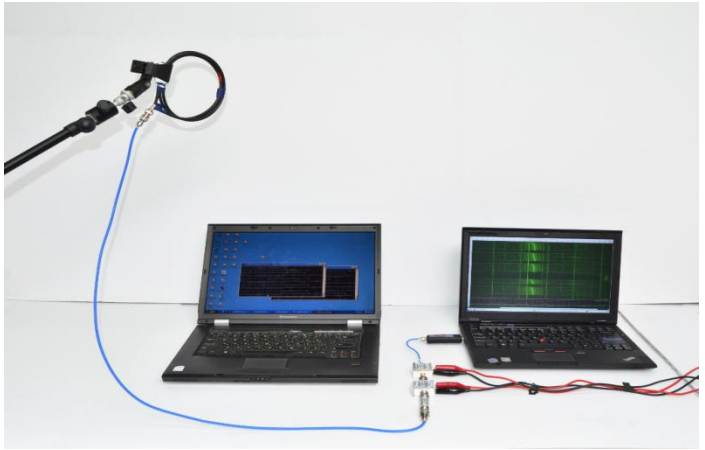
Abstract. By carefully measuring the amount of time required to perform private key operations, attackers may be able to find fixed Diffie-Hellman exponents, factor RSA keys, and break other cryptosystems. Against a vulnerable system, the attack is computationally inexpensive and often requires only known ciphertext. Actual systems are potentially at risk, including cryptographic tokens, network-based cryptosystems, and other applications where attackers can make reasonably accurate timing measurements. Techniques for preventing the attack for RSA and Diffie-Hellman are presented. Some cryptosystems will need to be revised to protect against the attack, and new protocols and algorithms may need to incorporate measures to prevent timing attacks.

Keywords: timing attack, cryptanalysis, RSA, Diffie-Hellman, DSS.

2.4. Análisis Emanaciones Electromagnéticas (*ElectroMagnetic Attack, EMA*)



Tradicionalmente, los EMA se han empleado para atacar tarjetas inteligentes, FGPA y otros dispositivos pequeños (PIC16F877).



Ataque a un portátil: antena, a 0.5 m. sobre el equipo a atacar, está conectada por un cable coaxial a un filtro de paso bajo y dos amplificadores.

- J.-J. Quisquater and D. Samyde, *Electromagnetic analysis (EMA): Measures and counter-measures for smart cards*. E-smart'01, 200-210, 2001.
- D. Genkin, L. Pacvhmanov, and I. Pipman, *Stealing Keys from PCs using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation*, Mar, 2015.

2.5. Análisis de Ruido (Sonido) (*Acoustics Attack*)

El micrófono del móvil (Samsung NOTE II), situado a 30 cm., apunta a los respiraderos del ventilador del portátil.

Micrófono parabólico, a 4 m., conectado a un portátil en un maletín acolchado ataca a otro portátil.

- D. Genkin, A. Shamir, and E. Tromer, *RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis*. Dec, 2013: "The attack can extract full 4096-bit RSA decryption keys from laptop computers, within an hour, using the sound generated by the computer during the decryption of some chosen ciphertexts (GnuPG)".

2.6. Análisis Físicos no invasivos (*non-invasive Physical Attack*)

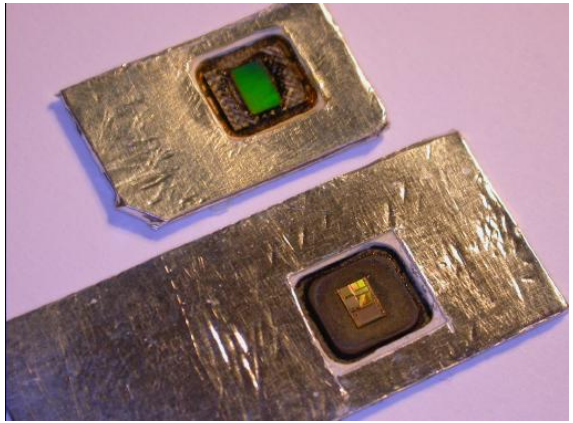
Fluctuaciones del potencial eléctrico del chasis de un portátil: con la toma de tierra o con un cable conductor conectado a un puerto I/O.

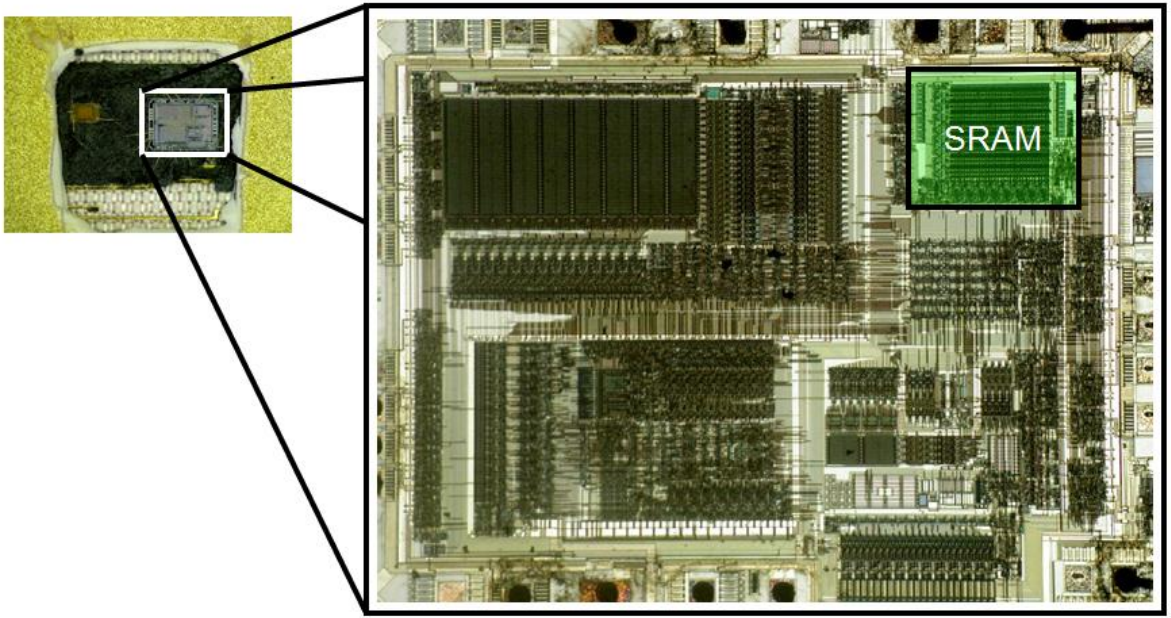
Tocando el equipo con la mano y midiendo el potencial del cuerpo

- D. Genkin, I. Pipman, and E. Tromer, *Get Your Hands O My Laptop: Physical Side-Channel Key-Extraction Attacks on PCs*. LNCS 8731, 242-260 (CHES 2014): "we have extracted 4096-bit RSA keys and 3072-bit ElGamal keys from laptops (GnuPG)".

2.7. Análisis por inducción de Fallos (*Fault Injection*)

Inducir fallos en determinadas zonas de memoria o en la ejecución de un algoritmo puede llevar a fugas para obtener la clave (ingeniería inversa)



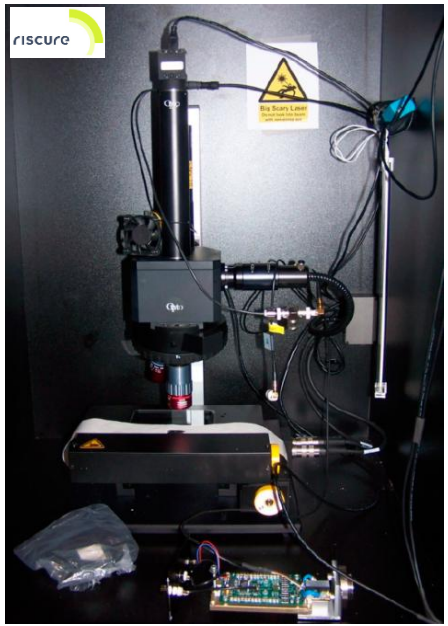


2.7. Análisis por inducción de Fallos (*Fault Injection*)

- DES y AES requieren desde unas docenas hasta unos cientos de fallos exitosos.
- RSA-CRT requiere sólo UN fallo exitoso (ataque de Bellcore, 2001).

Implementación eficiente de una firma:

- $d_p = d \bmod (p\text{-}1)$
- $d_q = d \bmod (q\text{-}1)$
- $P = p^{-1} \bmod q$
- $S_p = M^{dp} \bmod p$
- $S_q = M^{dq} \bmod q$
- $S = (((S_q\text{-}S_p)\cdot P) \bmod q)\cdot p + S_p$



Fallo corrompiendo S_q en un RSA-CRT: si $\mathbf{S}_q$ es un valor erróneo,

- $\mathbf{S} = (((\mathbf{S}_q\text{-}S_p)\cdot P) \bmod q)\cdot p + S_p$
- Restando $\mathbf{S}$ de S, resulta:
- $S - \mathbf{S} = (a\text{-}b)\cdot p \bmod n$

Calcular

- $\text{mcd}(S\text{-}\mathbf{S}, n) = \text{mcd}\ (a\text{-}b)\cdot p, p\cdot q) = p$
- Calcular $q = n/p$

3. Certificación de dispositivos

Para alcanzar un nivel adecuado de seguridad en una organización es preciso que, tanto los productos como los sistemas de las Tecnologías de la Información y Comunicaciones (TIC) utilizados, cuenten con unas características apropiadas, estén correctamente implementados y que, por otra parte, no realicen funciones indeseadas.

El único modo de asegurar que se cumplen estos requisitos es la realización de una evaluación[1] de la seguridad, realizada mediante la utilización de criterios rigurosos, con la posterior certificación[2] por parte del organismo legalmente establecido para ello.

En este sentido, el Centro Criptológico Nacional (CCN) actúa como Organismo de Certificación (OC) del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI), de aplicación a productos y Sistemas en su ámbito. Así lo estipula la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y el Real Decreto 421/2004, de 12 de marzo, por el que se regula el CCN.

Organismo de Certificación del CCN: OC-CCN

CERTIFICACIÓN FUNCIONAL

En base a criterios establecidos y reconocidos como estándar internacional (CC)

CERTIFICACIÓN CRIPTOLÓGICA

Productos capaces de proteger la información clasificada Nacional

CERTIFICACIÓN TEMPEST

Equipos y sistemas protegidos frente a las emanaciones electromagnéticas.

Common Criteria

SOGIS MRA

¿Cómo se certifica un producto STIC?

Productos Certificados

Certificación Funcional

Laboratorios Acreditados

Laboratorios Acreditados

Applus

- Qualified EAL1-4 for all products
- Qualified EAL1-7 for “Smartcards and similar devices”

Centro de Evaluación de la Seguridad de las Tecnologías de la Información (CESTI), del Instituto Nacional de Técnica Aeroespacial (INTA)

- CC: EAL4+ (AVA_VAN.5 y ALC_FLR.2)
- ITSEC/ITSEM: Hasta E4

Epoche and Espri

- Qualified EAL1-7 for “HW Devices with Security Boxes”

OC-CCN: miembro del Senior Officers Group for Information Systems, Mutual Recognition Agreement

SOGIS
Senior Officials Group
Information Systems Security

- Austria, Bundeskanzleramt
- Finlandia, FICORA - Finnish Communications Regulatory Authority
- Francia, ANSSI - Agence Nationale de la Sécurité des Systèmes d'Information
- Alemania, BSI - Bundesamt für Sicherheit in der Informationstechnik
- Italia, OCSI - Organismo di Certificazione della Sicurezza Informatica
- Países Bajos , NLNCSA - Netherlands National Communications Security Agency, Ministry of the Interior and Kingdom Relations
- Noruega, SERTIT - Norwegian National Security Authority operates the Norwegian Certification Authority for IT Security
- España, CCN - Centro Criptológico Nacional, Organismo de Certificación de la Seguridad de las Tecnologías de la Información
- Suecia, FMV - Försvarets Materielverk
- Reino Unido, CESG - Communications-Electronics Security Group

Muchas gracias por su atención

¿Preguntas?

E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sondas@ccn-cert.cni.es
- redsara@ccn-cert.cni.es
- organismo.certificacion@cni.es

Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

Síguenos en Linked in