CONDICIONS GENERALS D'ÚS

APLICABLES A

CERTIFICAT D'INFRAESTRUCTURA PERSONAL D'IDENTIFICACIÓ I SIGNATURA RECONEGUDA DE CLASSE 2 (CIPISR-2)

DE L'ENTITAT DE CERTIFICACIÓ

AGÈNCIA CATALANA DE CERTIFICACIÓ

(EC-ACC)

Control documental

Estat formal[1]	**Elaborat per:** Carlos Alonso	**Aprovat per:** Marta Cruellas
Data de creació	01/05/2010	
Control de versions	**Data:**	
	Descripció:	Creació
Nivell accés informació	pública	
Títol	Condicions Generals d'Ús del Certificat Infraestructura Personal d'Identificació i Signatura Reconeguda	
Fitxer	D1111 N-CGU CIPISR-2 EC-ACC v1r0 cat	
Control de còpies	Només les còpies disponibles a https://www.catcert.cat/ garanteixen l'actualització dels documents. Tota còpia impresa o desada en ubicacions diferents es consideraran còpies no controlades.	
Drets d'autor	Aquesta obra està subjecta a una llicència Reconeixement-No comercial-Sense obres derivades 2.5 Espanya de Creative Commons. Per veure'n una còpia, visiteu http://creativecommons.org/licenses/by-nc-nd/2.5/es/deed.ca o envieu una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.	

[1] Aquest document ha estat elaborat i aprovat internament a CATCert per les persones citades. L'aprovació definitiva ha estat realitzada pels òrgans designats a la Declaració de Pràctiques de Certificació corresponent.

Abans de verificar un certificat electrònic personal d'identificació i signatura reconeguda de classe 2 (en endavant, "CIPISR-2") de l'Entitat de Certificació "Agència Catalana de Certificació" (en endavant "EC-ACC"), o d'accedir o utilitzar la informació de l'estat de certificats i la resta de informació continguda en el Registre de EC-ACC, Vostè (en endavant, "el Verificador") ha de llegir i acceptar les presents Condicions Generals d'Ús (en endavant, "Condicions d'Ús").

La realització de qualsevol de les accions descrites en el paràgraf anterior implicarà que s'han acceptat, en la seva totalitat, les presents Condicions d'Ús.

Les condicions d'emissió del CIPISR-2, aplicables al subscriptor o al posseïdor de claus del certificat, es troben regulades en les "Condicions Generals d'Emissió" de EC-ACC aplicables.

En el supòsit de què el Verificador no estigui conforme amb la totalitat dels termes de les presents Condicions d'Ús haurà d'abstenir-se de realitzar qualsevol acció que guardi relació amb les clàusules aquí contingudes. En aquest cas, EC-ACC no assumeix responsabilitat alguna.

CLÀUSULES

PRIMERA.- *Objecte*

1.- Les presents Condicions d'Ús regulen la prestació per EC-ACC dels serveis de informació sobre els certificats, l'estat dels certificats i altres informacions publicades en el Registre de EC-ACC, en relació amb els certificats descrits en la clàusula tercera d'aquestes Condicions d'Ús.

2.- Aquestes Condicions d'Ús proporcionen garanties limitades al servei ofert, excloent qualsevol altre garantia i responsabilitat que no derivi del servei de certificació ofert al Verificador.

SEGONA.- *DPC i documentació d'operacions de EC-ACC*

1. La prestació dels Serveis de Certificació de EC-ACC es regula tècnica i operativament a la Declaració de Pràctiques de Certificació de EC-ACC (en endavant, la DPC) i les seves actualitzacions posteriors, així com en la documentació complementaria publicada en compliment del que disposen els articles 18 i 19 de la Llei 59/2003, de 19 de desembre, sobre signatura electrònica, en la següent adreça d'Internet: http://www.catcert.net/registre.

2. La DPC i la documentació d'operacions de EC-ACC, modificades periòdicament, s'incorporen a les presents Condicions d'Ús per referència. El Verificador declara conèixer la última versió de la DPC, els aspectes jurídics de la qual es contenen en les presents Condicions d'Ús.

3. El Verificador es compromet a complir amb els requisits tècnics, operatius i de seguretat descrits en la DPC i en la documentació d'operacions de EC-ACC.

4. En cas de discrepància, el significat dels termes continguts en les presents Condicions d'Ús prevaldrà sobre allò establert en la DPC.

TERCERA.- ***Descripció del CIPISR-2***

3.1. Naturalesa del Certificat

Els certificats d'infraestructura personal d'identificació i signatura reconeguda de classe 2 (CIPISR-2) són emesos a operadors del centre de trucades per les tasques de gestió del cicle de vida de certificats d'una Entitat de certificació.

Els certificats d'infraestructura d'identificació i signatura són certificats reconeguts d'acord amb el que s'estableix a l'article 11.1, amb el contingut prescrit per l'article 11.2 i emesos complint les obligacions dels articles 12, 13, i 17 a 20 de la Llei 59/2003, de 19 de desembre, de signatura electrònica.

Els CIPISR funcionen amb dispositiu segur de creació de signatura electrònica, d'acord amb l'article 24.3 de la Llei 59/2003, de 19 de desembre, i que donen compliment a allò disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions, identificada amb la referència TS 101 456.

Per aquest motiu, els CIPISR garanteixen la identitat del subscriptor i del posseïdor de la clau privada d'identificació i signatura, i permeten la generació de la "signatura electrònica reconeguda"; és a dir, la signatura electrònica avançada que es basa en un certificat reconegut i que ha estat generada emprant un dispositiu segur, per la qual cosa, d'acord amb el que estableix l'article 3 de la Llei 59/2003, de 19 de desembre, s'equipara a la signatura escrita per efecte legal, sense necessitat de complir cap altre requeriment addicional.

Els CIPISR són certificat d'operador i el seu ús exclusiu és l'operació dels components de la infraestructura de clau pública de CATCert com, per exemple, els components emprats per les Entitats de Registre Internes o Col·laboradores per aprovar i generar certificats, o per revocar-los, o pel servei d'atenció a usuaris per suspendre certificats.

Els CIPISR corresponents a l'Entitat de Certificació seran emesos per la pròpia Entitat de Certificació, amb l'aprovació prèvia de CATCert.

Els CIPISR corresponents a cada Entitat de Certificació Vinculada a l'Entitat de Certificació seran emesos per la pròpia Entitat de certificació, amb l'aprovació prèvia de l'Entitat de Certificació .

3.2. Finalitat i usos del Certificat

Els CIPISR-2 garanteixen la identitat del subscriptor i del posseïdor de la clau privada d'identificació i signatura, i permeten la generació de la "signatura electrònica reconeguda"; és a dir, la signatura electrònica avançada que es basa en un certificat reconegut i que ha estat generada emprant un dispositiu segur, per la qual cosa, d'acord amb el que estableix l'article 3 de la Llei 59/2003, de 19 de desembre, s'equipara a la signatura escrita per efecte legal, sense necessitat de complir cap altre requeriment addicional.

Per altra banda, els CIPISR-2 es poden utilitzar en aplicacions que no requereixen la signatura electrònica equivalent a la signatura escrita, sinó només la identificació del posseïdor de claus, en nom de la Institució, com les aplicacions que s'indiquen a continuació:

a. Autenticació en sistemes de control d'accés
b. Signatura de correu electrònic segur
c. Altres aplicacions de signatura digital

La signatura electrònica generada en l'ús d'aquestes aplicacions tindrà els efectes que en determini la normativa reguladora de l'aplicació, que podrà declarar l'equivalència amb la signatura escrita o només l'efecte d'identificació, ja que, si més no, aquesta signatura haurà estat produïda amb el dispositiu segur.

Els CIPISR-2 emesos per l'EC-ACC s'identifiquen amb l'identificador de l'objecte (OID):

OID: 1.3.6.1.4.1.15096.1.3.1.16

QUARTA.- *Llicència d'ús del Certificat*

4.1. Reserva de drets

Tots els continguts accessibles en relació amb la prestació dels serveis de certificació, el propi CIPISR-2, així com les especificacions, targetes, marques i demés aplicatius aparellats al seu ús estan subjectes a drets de propietat intel·lectual e industrial de EC-ACC o d'altres tercers titulars d'aquests.

En cap cas la prestació d'aquests serveis implica cap tipus de renuncia, transmissió o cessió total o parcial d'altres drets que els expressament reconeguts i atorgats en les presents Condicions d'Ús.

4.2. Llicència d'ús del CIPISR-2

EC-ACC atorga al Verificador llicència d'ús no exclusiva e intransferible del CIPISR-2 i de la informació d'estat d'aquests, amb la única i exclusiva finalitat de prestar-li els serveis i permetre l'ús del certificat de conformitat amb les presents Condicions d'Ús.

4.3. Inexistència de garantia de idoneïtat

EC-ACC no pot garantir que la utilització del CIPISR-2 i aplicatius informàtics aparellats permeti al Verificador l'obtenció o cobertura de necessitats, dades o fins de qualsevol índole, diferents als que poden assolir-se mitjançant el seu ús segons la seva pròpia naturalesa i segons el que es desprèn de la seva llicència d'ús.

4.4. Limitacions d'ús i usos prohibits

El CIPISR-2 només podrà ser utilitzat dins dels limites d'ús recollits de manera expressa a la seva llicència d'ús i en les presents Condicions d'Ús. Qualsevol altre ús fora dels descrits en la present clàusula queden expressament exclosos del present àmbit contractual i formalment prohibits.

El certificat no s'ha dissenyat, no es pot destinar i no s'autoritza el seu ús o revenda amb equips de control de situacions perilloses o per a usos que requereixen

actuacions a prova d'errors, amb el funcionament de instal·lacions nuclears, sistemes de navegació o comunicacions aèries, o sistemes de control d'armament, on un error pogués directament comportar la mort, lesions personals o danys mediambientals severs.

4.5. Duració de la llicència

La duració de la llicència d'ús del CIPISR-2 està limitada al termini màxim de validesa d'aquest, que és de quatre (4) anys.

La data d'inici de la vigència dels certificats ve determinada pel dia de la seva emissió, mentre que de la seva expiració figura indicada en el propi certificat, més enllà de qual no podrà utilitzar-se.

CINQUENA.- *Obligacions del Verificador*

5.1. Decisió informada

EC-ACC informa al Verificador, el qual es dona per notificat, que té accés a informació suficient per prendre una decisió informada en el moment de verificar un CIPISR-2 i confiar en la informació continguda en aquest.

De la mateixa forma, el Verificador reconeix que l'ús del Registre i de les Llistes de Revocació de Certificats (en endavant, "les LRCs" o "les LCRLs") de EC-ACC, es regeix per la DPC de EC-ACC i es compromet a complir els requisits tècnics, operatius i de seguretat descrits en l'esmentada DPC de EC-ACC.

5.2. Requisits de verificació de signatures electròniques.

Per confiar en una signatura electrònica, és imprescindible que el Verificador comprovi l'existència i la validesa tant del certificat com de la signatura electrònica, mitjançant l' execució del procediment de verificació.

La verificació implica comprovar l'autenticitat i la integritat del document electrònic signat, a fi de determinar que va ser generada per la EC legítima, que és la Agència Catalana de Certificació, utilitzant la clau privada corresponent a la clau pública continguda en el certificat del subscriptor, i que el document no va ser modificat des de la generació de la signatura electrònica.

La comprovació del certificat serà executada normalment de forma automàtica pel programari del Verificador i, en tot cas, de conformitat amb la DPC, amb els següents requisits ineludibles:

a) Utilitzar el programari apropiat per a la verificació de la signatura digital del CIPISR-2amb els algoritmes i longituds de claus autoritzats en el certificat i/o executar qualsevol altre operació criptogràfica, i establir la cadena de certificats en què es basa la signatura electrònica a verificar, ja que la signatura electrònica es verifica utilitzant aquesta cadena de certificats.

b) Assegurar que la cadena de certificats identificada és la més adequada per a la signatura electrònica que es verifica, ja que una signatura electrònica pot basar-se en més d'una cadena de certificats, i és decisió del Verificador assegurar-se d'utilitzar la cadena més adequada per verificar-la.

c) Comprovar l'estat de revocació dels certificats de la cadena amb la informació subministrada en el Registre de EC-ACC (Per exemple, la continguda en les LRCs) per determinar la validesa de tots els certificats de la cadena de certificats, doncs només pot considerar-se correctament verificada una signatura electrònica si tots i cada un dels certificats de la cadena són correctes i es troben vigents.

d) Assegurar que tots els certificats de la cadena autoritzen l'ús de la clau privada pel subscriptor del certificat i el posseïdor de la clau, degut a la possibilitat de què algun dels certificats inclogui límits d'ús que impedeixin confiar en la signatura electrònica que es verifica. Cada certificat de la cadena disposa d'un indicador que fa referència a les Condicions d'Ús aplicables, per a la seva revisió pels Verificadores.

e) Verificar tècnicament la signatura de tots els Certificats de la cadena abans de confiar en el Certificat utilitzat pel signatari.

f) Determinar la data i l'hora de generació de la signatura electrònica, ja que la signatura electrònica només pot considerar-se correctament verificada si ha estat creada dins el període de vigència de la cadena de certificats en què es basa.

g) Delimitar les dades que han estat signades digitalment, ja que aquestes s'utilitzaran en la verificació de la signatura.

h) Verificar tècnicament la pròpia signatura amb el certificat del signatari avalat per la cadena de certificats.

5.3. Diligència exigible

El Verificador ha de actuar amb la màxima diligència abans de confiar en un CIPISR-2. En concret, el Verificador s'obliga a utilitzar el programari de verificació de signatura electrònica amb la capacitat tècnica, operativa i de seguretat suficient per executar el procés de verificació de signatura correctament, i serà responsable exclusiu del dany que pugui sofrir per la incorrecta elecció de l'esmentat programari.

La prescripció anterior no serà aplicable quan EC-ACC hagi subministrat el programari de verificació al Verificador.

El Verificador pot confiar en un CIPISR-2 si concorren les condiciones següents:

a) La signatura electrònica s'ha de poder verificar d'acord amb els requisits establerts en l'apartat segon de la clàusula cinquena.

b) El Verificador ha de haver utilitzat informació de revocació actualitzada en el moment de verificar la firma.

c) El tipus i la classe de certificat té que ser l'apropiat per a l'ús que es pretén fer.

d) El Verificador ha de tenir en compte altres limitacions addicionals d'ús del certificat, indicades de qualsevol forma en el certificat, incloent aquelles no processades automàticament pel programari de verificació, incorporades per referència al certificat, i contingudes en aquestes Condicions d'Ús. En especial, un certificat no constitueix una concessió de drets i facultades per part de EC-ACC al subscriptor o al posseïdor de claus, més enllà de la descripció del certificat segons la clàusula tercera o una altra indicació expressa de EC-ACC o del propi subscriptor.

e) Finalment, la confiança ha de ser raonable d'acord amb les circumstancies. Si les circumstancies requereixen garanties addicionals, el Verificador haurà d'obtenir aquestes garanties per tal que la confiança sigui raonable.

En qualsevol cas, la decisió final amb respecte a confiar o no en un certificat CIPISR-2 verificat és exclusivament del Verificador, qui ha d'adoptar una actitud activa i al que se li exigeix l'accés a tota la informació disposada per EC-ACC per a prendre les seves decisions de forma totalment informada. En cas de dubte, el Verificador no ha de confiar en el CIPISR-2.

5.4. Confiança en una signatura no verificada

Queda prohibit confiar, o, de qualsevol altra forma, fer ús d'una signatura o certificat no verificats.

Si el Verificador confia en un certificat no verificat, assumirà tots els riscs derivats d'aquesta actuació.

5.5. Efecte de la verificació

En virtut de la correcta verificació d'una signatura i/o certificat CIPISR-2, de conformitat amb les Condicions d'Ús, el Verificador pot confiar en les dades del certificat o la CRL, dins de les limitacions d'ús corresponents.

5.6. Ús correcte i activitats prohibides

El Verificador s'obliga a no utilitzar cap classe de informació d'estat dels certificats o de cap altre tipus que hagi estat subministrada per EC-ACC, en la realització de qualsevol acte prohibit per la llei aplicable a aquest.

El Verificador s'obliga a no inspeccionar, interferir o realitzar enginyeria inversa en la implantació tècnica dels Serveis Públics de Certificació de EC-ACC, sense previ consentiment escrit de EC-ACC.

Addicionalment, el Verificador s'obliga a no comprometre intencionadament la seguretat dels Serveis Públics de Certificació de EC-ACC.

Els serveis de certificació digital prestats per EC-ACC no han estat dissenyats ni permeten la utilització o revenda, com equips de control de situacions perilloses o per

a usos que requereixen actuacions a prova d'errors, com l'operació de instal·lacions nuclears, sistemes de navegació o comunicació aèria, sistemes de control de tràfic aeri, o sistemes de control d'armament, on un error podria causar la mort, danys físics o danys mediambientals greus.

SISENA.- ***Obligacions de EC-ACC***

6.1. Relatives a la Prestació del Servei de Verificació de Certificats

EC-ACC s'obliga a la prestació del servei en determinades condicions tècniques i operatives, tal i com s'estableix en la DPC de EC-ACC, incloent un Registre de certificats, on es publica informació relativa a l'estat dels certificats.

EC-ACC s'obliga a emetre informació d'estat, incloent la suspensió i la revocació, dels certificats emesos, d'acord amb la DPC, així com a assumir les seves responsabilitats davant dels verificadores, sempre dins dels límits d'ús establerts pels certificats.

6.2. Garantia limitada de EC-ACC

EC-ACC garanteix al Verificador les condiciones del servei següents:

a) El Certificat CIPISR-2 conté informació correcta i actual en el moment de la seva emissió, degudament comprovada, de conformitat amb el que estableix la Llei 59/2003, de 19 de desembre.

b) El Certificat CIPISR-2 compleix tots els requisits relatius al contingut i al format establert a la DPC.

c) La clau privada de EC-ACC no ha estat compromesa, excepte notificació en contra mitjançant el Registre.

SETENA.- ***Règim de Responsabilitats***

7.1. Responsabilitat del Verificador

El Verificador respondrà per incompliment de les seves obligacions contractuals o per negligència.

El Verificador s'obliga a mantenir a EC-ACC indemne de qualsevol acte o omissió de la que resultin danys de tot tipus, incloent:

a) L'incompliment de les obligacions pròpies del Verificador.

b) La confiança en un certificat o signatura electrònica basada en aquest, que no sigui raonable.

c) L'incompliment de l'obligació de comprovar l'estat d'un certificat per a determinar si ha expirat o ha estat suspès o revocat.

7.2. Responsabilitat de EC-ACC

EC-ACC respondrà per incompliment de les obligacions que, en cada cas, imposa la Llei 59/2003, de 19 de desembre, sobre signatura electrònica o per negligència, excepte en els casos següents:

a) EC-ACC no serà responsable pels danys causats per les informacions contingudes en els certificats, sempre que aquestes siguin correctes i actuals en el moment de la emissió del certificat.

b) EC-ACC no serà responsable de cap dany directe o indirecte, especial, incidental, emergent, de qualsevol lucre cessant, pèrdua de dades, danys punitius, previsibles o imprevisibles, derivats de l'ús, enviament, llicència a tercers, funcionament o no funcionament dels certificats en un sistema no proporcionat per EC-ACC, així com de les signatures digitals o qualsevol altra transacció o servei descrit en la DPC, quan siguin utilitzats fora del Servei Públic de Certificació i els serveis de verificació de EC-ACC.

c) L'EC-ACC no serà en cap cas responsable de cap dany que resulti de cas fortuit o força major, com ara desastres naturals o disfuncions generals de les xarxes de telecomunicacions i solucions tecnològiques el funcionament de les quals no siguin responsabilitat de l'EC-ACC.

d) L'EC-ACC no respondrà dels danys o perjudicis derivats de l'acció d'un tercer.

e) L'EC-ACC no será responsable dels danys o perjudicis que pugui causar l'aplicació de normes legislatives o reglamentàries aprovades amb posterioritat a l'emissió d'aquestes Condicions Generals.

VUITENA.- Infracció de drets de tercers

CATCert no es responsabilitza de què l'enviament a CATCert, pel subscriptor o pel posseïdor de claus, per a la seva inclusió al certificat, així com la utilització d'un nom de domini i/o qualsevol altre tipus de nom o denominació, i la resta d'informació de sol·licitud dels certificats, infringeixi els drets de persona alguna en qualsevol jurisdicció respecte a les seves marques registrades, marques de servei, noms comercials o qualsevol altre dret de propietat intel·lectual o industrial, ni de què el subscriptor o el posseïdor de claus pretengui utilitzar el domini i els nom distingits per a cap propòsit il·legal, incloent-hi, sense limitació, la infracció amb dol d'un contracte, o l'obtenció de possibles avantatges comercials, la competència deslleial, la lesió del dret a l'honor, i la confusió o engany d'una persona, tant física com jurídica.

CATCert no es responsabilitza de la veracitat de la informació que li hagi estat comunicada pel subscriptor o pel posseïdor de claus, per a la seva inclusió als certificats emesos per CATCert, en jurisdicció qualsevol en la que aquesta informació es pugui utilitzar o visualitzar.

NOVENA.- ***Protecció de dades personals***

Determinades informacions relatives als certificats contenen dades de caràcter personal que han de protegir-se en atenció al que preceptua la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal.

El Verificador s'obliga a protegir les esmentades dades personals, així com a establir les adequades mesures de seguretat, de conformitat amb l'article 9 de la citada Llei Orgànica 15/1999.

En cas de què el Verificador rebi de EC-ACC qualsevol tipus de informació de caràcter personal en execució de les presents Condicions d'Ús, es compromet a utilitzar-la amb l'exclusiva finalitat de verificar la signatura del subscriptor del certificat. Així mateix, s'obliga a no utilitzar aquestes dades per a qualsevol altre fi, sense el consentiment exprés del subscriptor.

El Verificador serà responsable exclusiu de les incidències derivades de la infracció d'aquestes obligacions de protecció de dades personals, obligant-se a mantenir indemne a EC-ACC de tot dany derivat d'aquestes incidències.

DESENA.- ***Divisibilitat de les Condicions d'ús***

Les clàusules de les presents Condicions d'ús són independents entre sí, motiu pel qual si qualsevol clàusula és considerada invàlida o inaplicable, la resta de clàusules de les presents Condicions d'ús seguiran sent aplicables, excepte acord exprés en contrari de les parts.

ONZENA.- ***Finalització de la relació jurídica i supervivència de determinades obligacions***

10.1. Aquestes Condicions d'ús finalitzaran quan acabi la llicència d'ús del certificat que es concedeix, i de forma anticipada per infracció, per qualsevol de les parts, de les seves obligacions establertes en la Declaració de Pràctiques de Certificació.

10.2. Les següents obligacions de la Declaració de Pràctiques de Certificació romandran vigents per ambdues parts durant un termini màxim de dos anys des de la finalització d'aquest contracte: Obligacions i responsabilitat civil (secció 9.6 de la DPC), auditoria de conformitat (secció 8 de la DPC), i confidencialitat (9.4). Les obligacions derivades de la protecció de dades personals romandran mentre no es cancel·lin les dades personals, d'acord amb la normativa vigent.

DOTZENA.- ***Notificació***

Totes les modificacions que l'EC-ACC realitzi sobre aquestes condicions generals seran notificades a través del la pàgina web de l'EC-ACC indicada a la clàusula segona d'aquestes condicions generals.

El verificador ha de remetre qualsevol notificació en relació amb aquestes condicions generals a les adreces de l'EC-ACC indicades a la pàgina web de l'EC-ACC.

TRETZENA.- ***Legislació aplicable i jurisdicció competent***

Les presents Condicions d'ús seran interpretades i executades en els seus propis termes i, en tot allò no previst, les parts es regiran per la Llei 59/2003, de 19 de desembre, per la legislació administrativa aplicable i, subsidiàriament, per la legislació civil i mercantil que regula el règim de les obligacions i dels contractes.

La jurisdicció competent és la que s'indica en la Llei 29/1998, de 13 de juliol, reguladora de la Jurisdicció Contenciosa Administrativa.