

Universitat Rovira i Virgili

Instal·lació de claus públiques

Servei de Recursos Informàtics i TIC



Sumari

Objectius del document1
Jerarquia d'entitats de certificació de CATCert1
Instal·lació de claus públiques2
Mozilla Firefox2
Internet Explorer



Objectius del document

El present document descriu els procediments a seguir per tal d'instal·lar els certificats digitals de les entitats de certificació de la jerarquia de l'Agència Catalana de Certificació (CATCert), a la que pertany l'entitat de certificació de la Universitat Rovira i Virgili, en un ordinador basat en sistema operatiu Windows de Microsoft i amb la possibilitat d'utilitzar tant el navegador de Microsoft Internet Explorer versió 5 o superior, com el navegador de Mozilla Firefox versió 1.5 o superior.

Jerarquia d'entitats de certificació de CATCert

La jerarquia d'entitats de certificació de CATCert, l'arrel de la qual és la pròpia Agència, actualment s'estructura d'acord amb el diagrama que es mostra a la Figura 1.



Figura 1

La creació d'aquesta infrastructura si bé és necessària no és suficient i es fa necessari que els diferents usuaris explícitament hi confiïn. Els navegadors dels equips ja incorporen la confiança en algunes entitats de certificació. Per comprovar quines són aquestes entitats s'han d'executar les següents opcions als diferents navegadors:

Microsoft Internet Explorer

menú *Herramientas*, opció *Opciones.de Internet.*, secció *Contenido*, botó *Certificados*, pestanya *Entidades emisoras de certificados de raiz de confianza* (veure EC-ACC) i pestanya *Entidades emisoras de certificados intermedias* (veure EC-UR i EC-URV). [Figures 14 i 15]

Mozilla Firefox

Menú *Eines*, opció *Opcions...*, secció *Avançat*, pestanya *Xifratge*, botó *Visualitza els certificats*, pestanya *Entitats* i veure els certificats d'EC-ACC, EC-UR i EC-URV carregats. [Figura 5]

Les claus públiques de les entitats de certificació de la jerarquia de CATCert, entre les que es troba l'EC-URV, encara no venen precarregades als navegadors. CATCert acompleix tots els requisits necessaris perquè s'incloguin les claus públiques de les entitats de la seva jerarquia en els navegadors més coneguts. Aquest tràmit ja ha estat endegat per part de CATCert i s'estan realitzant els treballs necessaris per tal d'aconseguir-ho el més aviat possible. Mentre se segueix aquest procés cal instal·lar manualment aquestes claus.

És necessari instal·lar les claus de les tres entitats de certificació que formen la branca a la que pertany l'EC-URV per a que la ruta de certificació estigui completada quan els diferents programaris comprovin l'arbre de certificació.

Instal·lació de claus públiques



Instal·lació de claus públiques

Mozilla Firefox

Les claus públiques estan disponibles a l'apartat *Descàrrega de claus públiques* del web del Servei de Certificació Digital <u>http://www.urv.cat/scd</u>. [Figura 2]





Per instal·lar-les simplement s'ha de fer clic a cadascun dels enllaços. Es mostrarà un quadre de diàleg per confiar en una nova entitat de certificació. [Figura 3]

Baixada de certificats	×
Se us ha demanat que confieu en una entitat certificadora (CA) nova.	
Voleu confiar en «EC-ACC» per a les finalitats següents?	
🗖 Confia en aquesta CA per a identificar llocs web.]
🔲 Confia en aquesta CA per a identificar usuari de correu electrònic.	
🔲 Confia en aquesta CA per a identificar desenvolupadors de programari.	
Abans de confiar en aquesta CA amb qualsevol finalitat, cal que n'examineu el certificat i les norme i procediments (si estan disponibles).	s
Visualitza Examina el certificat de la CA	
D'acord Cancel·la	

Figura 3

S'han de seleccionar les tres opcions de la pantalla i prèmer el botó *D'acord*. [Figura 4]

Baixada de certificats	×
Se us ha demanat que confieu en una entitat certificadora (CA) nova.	
Voleu confiar en «EC-ACC» per a les finalitats següents?	
🔽 Confia en aquesta CA per a identificar llocs web.	
🔽 Confia en aquesta CA per a identificar usuari de correu electrònic.	
🔽 Confia en aquesta CA per a identificar desenvolupadors de programari.]
Abans de confiar en aquesta CA amb qualsevol finalitat, cal que n'examineu el certificat i les normes i procediments (si estan disponibles).	5
Visualitza Examina el certificat de la CA	
D'acord Cancel·la	



Per comprovar que s'han instal·lat correctament, s'ha d'accedir al menú *Eines*, opció *Opcions...*, secció *Avançat*, pestanya *Xifratge*, botó *Visualitza els certificats*, pestanya *Entitats* i veure els certificats d'EC-ACC, EC-UR i EC-URV carregats. [Figura 5]

🥹Gestor de certificats	
Els vostres certificats D'altri Servidors Entitats Altres	
Teniu certificats al fitxer que identifiquen aquestes entitats certificadores:	
Nom del certificat Dispositiu de seguretat	
AddTrust Qualified CA Root Builtin Object Token	
🗖 Agencia Catalana de Certificacio (NIF Q-0801176	
EC-IDCat Dispositiu de seguretat de progr	
EC-UR Dispositiu de seguretat de progr	
EC-URV Dispositiu de seguretat de progr	
EC-ACC Dispositiu de seguretat de progr	
🖃 America Online Inc.	
America Online Root Certification Authority 1 Builtin Object Token	
America Online Root Certification Authority 2 Builtin Object Token	
AOL Time Warner Inc.	
AOL Time Warner Root Certification Authority 1 Builtin Object Token	
Visualitza Edita Importa Exporta Suprimeix	

Figura 5

Si ja es tenen les claus públiques instal·lades, quan s'intenten instal·lar es mostra el missatge de la Figura 6.





Internet Explorer

Les claus públiques estan disponibles a l'apartat *Descàrrega de claus públiques* del web del Servei de Certificació Digital <u>http://www.urv.cat/scd</u>. [Figura 7]

🕲 Descàrrega de claus públiques - Mozilla Firefox	_ 🗆 ×
	0 ⁰ 0 000 000
C X 🔥 😰 http://www.aurv.net/la_urv/10_serveis/ritic/scd/certificats_digitals/descarrege 🟠 🔹 💽 Google	
🖉 Més visitades 🦆 Comenzar con Firefox 🔊 Ultimas noticias 🗇 coreu.urv.cat 🗭 Universitat Rovira i Vi 🧭 Universitat Rovira i Vi 🎍 Identity	Manager - C
Descàrrega de claus públiques	-
	•
Les claus públiques de les entitats de certificació són necessàries per verificar que els certificats que arriben als nostres equips informàtics han estat emesos per alguna de les autoritats de certificació de la jerarquia d'entitats de CATCert.	
La jerarquia actual d'entitats de certificació de CATCert està estructurada d'acord amb el diagrama següent:	
CATCert	
Agència Catalana Agència Catalana	
GENERALITAT DE CATALUNYA CIUTADÀNA ADMINISTRACIÓ UNMERSITATS PARLAMENT LOCAL I RECERCA DE CATALUNYA	
SAFP Generalitat i DiputAcions DIPUTACIONS CESCA URV PARLAMENT	
E-Red Ausside	
Entitat de certificació	
Certificació arrel	
Autoro fontane la Continue	
Els navegadors porten incorporada per defecte la confiança en algunes entitats de certificacio. Per comprovar quines son aquestes entitats s'han d'executar les següents opcions als diferents navegadors:	
Microsoft Internet Explorer Manú Sinas > aprió Opcians d'Internet > pastapus Contingut > baté Cartificate >> pastapus Entitate emissiones de cartifica	+-
arrel de confiança.	
Mozilla Firefox Menú Eines -> opció Opcions> secció Avançat, pestanya Xifratge, botó Visualitza els certificats, pestanya Entitats.	
Les claus públiques de les entitats de certificació de la jerarquia de CATCert, entre les que es troba l'EC-URV, encara no	
venen precarregades als navegadors. CATCert acompleix tots els requisits necessaris perquè s'incloguin les claus públiqu de les entitats de la seva jerarquia en els navegadors més coneguts. Aquest tràmit ja ha estat endegat per part de	25
CATCert i s'estan realitzant els treballs necessaris per tal d'aconseguir-ho el més aviat possible. Mentre se segueix aques procés cal instal·lar manualment aquestes claus.	t
És necessari instal·lar les claus de les tres entitats de certificació que formen la branca a la que pertany l'EC-URV. Es pode descarregar des dels següents enllaços:	'n
Arrel de l'Agència Catalana de Certificació (CATCert)	
Entitat de Certificació d'Universitats i Recerca	
Entitat de Certificació de la URV	
A l'apartat Suport - Manuals hi ha disponible el manual que descriu el procés d'instal·lació d'aquestes claus als diferents navegadors.	
\odot	-
Fet	•
	00 11

Figura 7



Per instal·lar-les simplement s'ha de fer clic a cadascun dels enllaços. Es mostrarà un quadre de diàleg on cal seleccionar l'opció Abrir. [Figura 8]

Descarga	de archivos		×
?	Algunos archivos pueden o abajo, parece sospechosa ni guarde este archivo.	dañar su equipo. Si la información del archivo, más o no confía plenamente en el origen de él, no abra	
	Nombre de archivo:	EC-ACC.ort	
	Tipo de archivo:	Certificado de seguridad	
	De:	wwwa.urv.net	
	Este tipo de archivo p código malicioso.	uede dañar su equipo si es que contiene	
	¿Desea abrir el archivo o g	uardarlo en su equipo?	
	<u>Abrir</u> <u>G</u> uard	dar Cancelar <u>M</u> ás información	
	Preguntar siempre ante	s de abrir este tipo de archivos	

Figura 8

Es mostrarà una nova finestra on es detallarà la informació de la clau pública on s'ha de seleccionar l'opció *Instalar certificado...* [Figura 9]

Certificado	<u>?</u> ×
General Detalles Ruta de certificación	
Información del certificado	
Qué hace este certificado:	- 11
Asegura la identidad de un equipo remoto Prueba su identidad a un equipo remoto Confirma que el software procede de una compañía de software Protege el software de alteraciones después de su	
* Más info. en declaración de entidades emisoras de certificados.	_
Enviado a: EC-ACC	
Emitido por EC-ACC	
Válido desde 08/01/2003 hasta 08/01/2031	
Instalar certificado Declaración del emi	sor
Ace	eptar



Es mostrarà la pantalla de la Figura 10.

Asistente para importación de	e certificados	×
	Éste es el Asistente para importación de certificados	
	< <u>A</u> trás Siguiente > Cancela	r

Figura 10

S'ha de seleccionar el botó *siguiente* i es mostrarà la pantalla de la Figura 11, on s'han de mantenir les opcions marcades per defecte i seleccionara el botó *siguiente*.



sistente pa	ra importación de certificados	x
Almacén	de certificados	
Los almac	enes de certificados son áreas del sistema donde se guardan los certificados.	
Windo posible	ws puede seleccionar automáticamente un almacén de certificados, o bien es e especificar una ubicación para el certificado.	_
c	Seleccionar automáticamente el almacén de certificados en base al tipo de certificado	
0	Colocar todos los certificados en el siguiente almacén	
	Almacén de certificados:	
	E <u>x</u> aminar	
	< <u>A</u> trás <u>Sig</u> uiente > Cancelar	

Es mostrarà la pantalla de la Figura 12, on s'informa de la finalització del procés.

Asistente para importación d	e certificados	×
	Finalización del Asistente para importación de certificados	
	Ha completado con éxito el Asistente para importación de certificados. Ha especificado la siguiente configuración:	
	Almacén de certificados seleccionado Determinado de fo Contenido Certificado	
	< <u>A</u> trás Finalizar Cancela	ar 🔤





Per comprovar que s'han instal·lat correctament, s'ha d'accedir al menú *Herramientas*, opció *Opciones.de Internet.*, secció *Contenido*, botó *Certificados*, pestanya *Entidades emisoras de certificados de raiz de confianza* (veure EC-ACC) i pestanya *Entidades emisoras de certificados intermedias* (veure EC-UR i EC-URV). [Figures 14 i 15]

Certificados					? ×
Propósito planteado:	<tod< th=""><th>os></th><th></th><th></th><th>•</th></tod<>	os>			•
Entidades emisoras de	certifi	icados de raíz de confianza			
Emitido para		Emitido por	Fecha de	Nombre descriptivo	
🔛 DSTCA E2		DSTCA E2	09/12/2018	DSTCA E2	
DST-Entrust GTI	CA	DST-Entrust GTI CA	09/12/2018	DST-Entrust GTI	
EC-ACC		EC-ACC	08/01/2031	<ninguno></ninguno>	
Entrust.net Certi	fic	Entrust.net Certificati	24/12/2019	Entrust.net Certi	
Entrust.net Clien	t C	Entrust.net Client Cer	12/10/2019	Entrust.net Clien	
Entrust.net Clien	t C	Entrust.net Client Cer	07/02/2020	Entrust.net Glob	
Entrust.net Secu	re	Entrust.net Secure Se	25/05/2019	Entrust.net Secu	
Entrust.net Secu	re	Entrust.net Secure Se	04/02/2020	Entrust.net Glob	
Equifax Secure C	ert	Equifax Secure Certifi	22/08/2018	Equifax Secure	-
Importar Expo	rtar del ce	. Quitar		Avanza	das
				<u>V</u> er	rar



ertificados P <u>r</u> opósito planteado: <a>	os>			?
Personal Otras personas	Entidades emisoras de cerl	tificados intern	nedias Entic	lades emi 💶 🕨
Emitido para	Emitido por	Fecha de	Nombre des	scriptivo 🔺
🔤 AddTrust External	UTN-USERFirst-Hardw	09/07/2019	<ninguno></ninguno>	
E CPX-1 C Antonio Co	EC-URV	19/02/2011	<ninguno></ninguno>	
CPX-1 C Jordi Tomà	EC-URV	29/03/2010	<ninguno></ninguno>	
🖾 EC-UR	EC-ACC	17/12/2019	<ninguno></ninguno>	
EC-URV	EC-UR	03/05/2013	<ninguno></ninguno>	
Enviament correus	EC-URV	23/05/2012	<ninguno></ninguno>	
GlobalSign Root CA	Root SGC Authority	28/01/2014	<ninguno></ninguno>	
GTE CyberTrust Root	Root SGC Authority	23/02/2006	<ninguno></ninguno>	
Microsoft Windows	Microsoft Root Authority	31/12/2002	<ninguno></ninguno>	•
Importar	. Quitar			<u>A</u> vanzadas
-Propósitos planteados del ce	ertificado			
<todos></todos>				
			_	<u>V</u> er
				<u>⊂</u> errar