Validação de Assinatura Digital

Quando um documento PDF assinado digitalmente é recebido, o processo de validação tende a decorrer automaticamente no Adobe Reader. Atendendo contudo às múltiplas versões existentes, e às diferentes configurações por defeito que foram existindo ao longo do tempo, pode ser necessário alterar configurações para uma correta validação.

O processo de validação das assinaturas digitais decorre em diversas etapas, das quais as mais fundamentais são as seguintes:

- Verificação de que o certificado de assinatura é de confiança
- Verificação que o documento está corretamente assinado e não foi adulterado
- Verificação da validade das datas de assinatura

Quando um documento PDF está assinado digitalmente, a sua visualização é acompanhada de uma inscrição que refere que o documento está corretamente assinado:



Para visualizar mais detalhes sobre a assinatura digital, é preciso clicar no icon referente às assinaturas digitais, conforme se pode ver na imagem abaixo. Aí será possível observar todos os detalhes da assinatura. Neste caso, confirme que a assinatura é efetuada por "Banco Santander Totta, S.A":



Problemas de verificação

As diferentes versões de Adobe Reader têm particularidades que podem fazer com que a assinatura digital não seja automaticamente reconhecida. Quando tal acontece, é habitual surgir um alerta semelhante ao visualizado na imagem seguinte:

Arguivo	cod_acesso_signed20170316125857701_00794.pdf - Ado Editar <u>Vi</u> sualizar Ja <u>n</u> ela Ajuda	be Acro	bat Re	ader DC			
Iníci	io Ferramentas cci_cod_acesso_sign �	1	k	٢	⊝ ⊕	73,4%	· B
	Assinaturas X Er Validar todas			٩	Santan	der Tot	ta Ne Em
¢.	Rev. 1: Assinado por Banco Suntander Totta, S.A. Va idade da assinatura desconhecida: O documento não foi modificado desde que e: A identidade do signatário é desconhecida, poi O horário de assinatura é o que consta no com			Junto seu ci O seu CORI Os se Nome Códig	o enviamos as cr artão u cartão PORATE INDIV sus dados de ac e de utilizador: go de acesso: úl	redenciais para /IDUAL GOLD esso timos ó dígitos	que possa acede do seu cartão
	Cinque para exiún esta versau	•		Aced Aced No pr	er ao Site do Sa a a santanderto rimeiro login e p	antander Totta otta.pt e no can oor motivos de :	to superior direit segurança, será s

Para verificar a correção da assinatura digital, deverá verificar que a configuração está adequada. O processo é distinto no caso das várias versões do Adobe Reader. De seguida, apresentam-se as configurações das três versões mais recentes¹, uma em Português e duas outras em Inglês. Em qualquer um dos casos, pode ser necessário reiniciar o Adobe Reader, para que as alterações surtam efeito.

¹ https://en.wikipedia.org/wiki/Adobe_Acrobat_version_history

Adobe Reader DC

Em "Editar"->"Preferências", na categoria "Assinaturas", em "Verificação", verificar que os seguintes pontos estão configurados:

- Em "Comportamento de verificação", desselecionar a opção "Exigir que a verificação de anulação do certificado seja feita sempre que possível ao verificar assinaturas".
- Em "Horário da verificação", "Verificar assinaturas usando:", selecionar a opção "Hora na qual a assinatura foi criada".
- Em "Integração com o Windows", "Confiar em TODOS os certificados raiz no Repositório de certificados do Windows para:", selecionar a opção "Validando assinaturas".

Quando o documento possui assinaturas válidas mas não confiáveis, avisa	ar para revisar e confiar nos signatários
Comportamento de verificação Ao verificar: Usar o método especificado pelo documento; avise se indisponível Usar o método especificado pelo documento. Se indisponível, use Sempre usar o método padrão: Exigir que a verificação de anulação do certificado seja feita sempre qu Usar marcas de data/hora vencidas	el : o método padrão • • ve possível ao verificar assinaturas
Ignorar as informações de validação do documento	
Horário da verificação	Informações de verificação
Verificar assinaturas usando: Hora na qual a assinatura foi griada Jempo de segurança (carimbo de data/hora) incorporado na assinatura Hora atual 	Adicionar automaticamente informações de verificação ao salvar um PDF assinado:
	() Handa
Integração com o Windows Confiar em TODOS os certificados raiz no Repositório de certificados do V Validando agsinaturas Validando gocumentos certificados A seleção de uma destas opções pode resultar no tratamento de mate	Vindows para: erial arbitrário como conteúdo

Adobe Reader XI

Em "Edit"->"Preferences", na categoria "Signatures", em "Verification", verificar que os seguintes pontos estão configurados:

- Em "Verification Behavior", desselecionar a opção "Require certificate revocation to succeed whenever possible during signature verification".
- Em "Verification Time", "Verify Signatures Using:", selecionar a opção "Time at which the signature was created".
- Em "Windows Integration", "Trust ALL root certificates in the Windows Certificate Store for:", selecionar a opção "Validating Signatures".

ignature Verification Preferences	
✓ Verify signatures when the document is opened	
When document has valid but untrusted signatures, prompt to review and trust signers	
┌─Verification Behavior	
When Verifying:	
○ Use the document-specified method; prompt if unavailable	
Use the document-specified method; if unavailable, use default method	
C Always use the default method: Adobe Default Security	
Require certificate revocation checking to succeed whenever possible during signature verifica	ion
Ignore document validation information	
-Varification Time-	
Verify Signatures Using:	
Time at which the signature was created	
Secure time (timestamp) embedded in the signature	
O Current time	
V Use envirod timestames	
(Ose <u>Expired an estamps</u>	
Verification Information	
Automatically add verification information when saving signed PDF:	
Ask when verification information is too big	
C Always	
O Never	
Windows Integration	
Trust ALL root certificates in the Windows Certificate Store for:	
Validating Signatures	
□ Validating Certified <u>D</u> ocuments	
Selecting either of these options may result in arbitrary material being treated as trusted cont Take care before enabling these features.	nt.
Help OK C	ancel

Adobe Reader 10

Em "Edit"->"Preferences", na categoria "Security", clicar em "Advanced Preferences":

Lategories:	Digital Signatures	
Commenting		
Documents	v verify signatures when the document is opened	vanced Preferences
Full Screen	View documents in preview document mode when signing	
General	Anno1739.50	
Page Display	Appendice	New
3D & Multimedia		<u>I4</u> CVV
Accessibility		Edit
Forms		
Identity		Duplicate
International		
Internet		Delete
JavaScript		
Measuring (2D)		
Measuring (2D) Measuring (3D)		
Measuring (2D) Measuring (3D) Measuring (Geo)	Security Settings	
Measuring (2D) Measuring (3D) Measuring (Geo) Multimedia (legacy)	Security Settings	
Measuring (2D) Measuring (3D) Measuring (Geo) Multimedia (legacy) Multimedia Trust (legacy)	Security Settings Duad security settings from a server Server Settings	
Measuring (2D) Measuring (3D) Measuring (Geo) Multimedia (legacy) Multimedia Trust (legacy) Online Services	Security Settings C Load security settings from a server Server Settings URL:	
Measuring (2D) Measuring (3D) Measuring (Geo) Multimedia (legacy) Multimedia Trust (legacy) Online Services Reading	Security Settings Coad gecurity settings from a server Server Settings URL:	
Measuring (2D) Measuring (3D) Measuring (Geo) Multimedia (legacy) Multimedia Trust (legacy) Online Services Reading Reviewing	Security Settings C Load gecurity settings from a server Server Settings UBL: Settings must be signed by: Allow Any Certificate	v Browse
Measuring (2D) Measuring (3D) Measuring (Geo) Multimedia (legacy) Multimedia Trust (legacy) Online Services Reading Reviewing Search Search	Security Settings C Load security settings from a server Server Settings UBL: Settings must be signed by: Allow Any Certificate	* Browse
Measuring (2D) Measuring (3D) Measuring (Geo) Multimedia (legacy) Multimedia Trust (legacy) Online Services Reading Reviewing Search Security Security	Security Settings Cad gecurity settings from a server Server Settings UBL: Settings must be signed by: Chlow Any Certificate Check every: Week Month	Browse Update Now
Measuring (2D) Measuring (3D) Measuring (Geo) Multimedia (legacy) Multimedia Trust (legacy) Online Services Reading Reviewing Search Security Security (Enhanced) Security (Enhanced)	Security Settings CLoad security settings from a server Server Settings UBL: Settings must be signed by: Allow Any Certificate Check every: Week Month	Browse Update Now
Measuring (2D) Measuring (3D) Measuring (Geo) Multimedia (legacy) Multimedia Trust (legacy) Online Services Reading Reviewing Search Security Security Security Security (Enhanced) Spelling Tracker	Security Settings County Settings from a server Server Settings UBL: Settings must be signed by: Allow Any Certificate Check every: Week Month 2 Week Allow Any Ask before updating	Browse Update Now
Measuring (2D) Measuring (3D) Measuring (Geo) Multimedia (legacy) Multimedia Trust (legacy) Online Services Reading Reading Reaviewing Search Security Security (Enhanced) Spelling Tracker Trust Manager	Security Settings Cad gecurity settings from a server Server Settings UBL: Settings must be signed by: Chlow Any Certificate Check every: 2 Week 3 Month 2 Week 3 Month Ask before updating	Browse Update Now
Measuring (2D) Measuring (3D) Measuring (Geo) Multimedia (Iegacy) Multimedia Trust (Iegacy) Online Services Reading Reviewing Seavich Security Security Security (Enhanced) Spelling Tracker Trust Manager Units	Security Settings Cad gecurity settings from a server URL: Settings must be signed by: Allow Any Certificate Check every: Week Month 2 Week Allow Any Certificate	Browse Update Now
Measuring (2D) Measuring (3D) Measuring (Geo) Multimedia (legacy) Multimedia Trust (legacy) Online Services Reading Reviewing Security Security Security Security Security Security Security Trust Manager Units Updater	Security Settings Career Settings UBL: Setti	Browse Update Now
Measuring (2D) Measuring (3D) Measuring (Geo) Multimedia (Iegacy) Online Services Reading Reviewing Search Security Security Security Security Spelling Tracker Trust Manager Units Updater	Security Settings Clad gecurity settings from a server Server Settings UBL: Settings must be signed by: Chlow Any Certificate Check every: Veek Month 2 Week Allow Any Certificate Check every: Allow Any Certificate Check every: Clear remembered account information	Browse Update Now

Na janela que se segue, verificar que os seguintes pontos estão configurados na pasta "Verification":

- Desselectionar a opção "Require certificate revocation checking to succeed whenever possible during signature verification".
- Em "Verification Time", "Verify Signatures Using:", selecionar a opção "The time at which

the signature was created".

Ve	rification	Creation	Windows Integrati	ion						
	When Veri	fying:								
	<u>ال</u> و	e the docu	iment-specified met	thod. Prompt if it is not	available.					
	Use the document-specified method. Use the default method if it is not available.									
	Alv	<u>v</u> ays use th	he default method (overrides the documen	t-specified met	hod).				
	De <u>f</u> ault Me	ethod for V	/erifying Signatures:	Adobe Default Secu	rity 👻					
	🔲 <u>R</u> equire	certificate	e revocation checkir	ng to succeed wheneve	r possible durin	g signature verifica	tion			
	Ignore (document	validation informat	tion						
	Verificati	on Time								
	Verify S	ignatures	Using:							
	0	The currer	nt time							
	Secure time (e.g. timestamp) embedded in the signature if available, current time otherwise									
	0	The <u>t</u> ime a	at which the signatu	ure was created						
		Use <u>expire</u>	ed timestamps							

Na pasta "Windows Integration", verificar que os seguintes pontos estão configurados:

- Seleccionar "Enable searching the Windows Certificate Store for certificates other than yours".
- Abaixo de "Trust ALL root certificates in the Windows Certificate Store for the following operations:", selecionar a opção "Validating Signatures".

Digital Sign	atures Advanced	Preferences				
Verifica	tion Creation	Windows Integration				
En	able searching th	e Windows Certificate	Store for <u>c</u> ertificate	es other than yours		
Trust	ALL root certifica	tes in the Windows Ce	ertificate Store for t	he following operatio	ons:	
	Validating Sign	atures				
	Validating Certi	fied <u>D</u> ocuments				
4	If either of the installed in Withis feature.	ese options are selecto /indows may be treate	ed content from co ed as trusted conter	mpanies that have co ht. Care should be tak	ertificates ken in enabling	
Help	>				ОК	Cancel

Validação em Linux

Em Linux, apesar de ser possível abrir um PDF assinado, não é possível normalmente verificar a sua autenticidade. Os leitores habituais (eg. Evince, Foxit Reader) não suportam a verificação da autenticidade de um documento PDF. O poppler, a partir da versão 0.42², inclui algum suporte para validação de assinaturas PDF, mas deve ser considerado experimental.

O Adobe Reader já não é suportado, dado que a última versão existente é de 2013. O seu download ainda é todavia possível³. Não se recomenda a sua utilização, dado ser software desatualizado e não suportado, mas por razões de completude, a verificação de um PDF assinado digitalmente, em Adobe Reader 9 para Linux, é muito semelhante para a versão Windows.



Validação em OS X

Existem apps pagas que anunciam a verificação do processo de assinatura, mas as mesmas não foram validadas. Um exemplo é o PDF Signet⁴.

Validação em Android

Os leitores gratuitos de PDF em Android (Adobe Reader, Google PDF Viewer) não suportam a verificação da autenticidade de assinaturas digitais de um documento PDF.

Algumas apps pretendem efetuar a validação de um PDF assinado, mas falham frequentemente, devido a vários fatores, incluindo o não suporte de algoritmos mais recentes (eg. SHA2). Tal é o caso por exemplo do OfficeSuite pro⁵.

² https://poppler.freedesktop.org/releases.html

³ ftp://ftp.adobe.com/pub/adobe/reader/unix/9.x/9.5.5/

⁴ https://pdfsignet.com/

⁵ erro:"Not supported signature type"

Validação em iOS

Os leitores gratuitos de PDF em iOS (Preview, Adobe Reader) não suportam a verificação da autenticidade de assinaturas digitais de um documento PDF.

Outras apps pagas dizem suportar a validação de assinaturas digitais, como é o caso de Software602 Signer⁶, mas o número de permissões requerida, bem como a forma de validação, sugerem fortemente a sua não utilização.

⁶ https://www.602.cz/en/about-us/download/supported-products/signer/