

Video Authentication Manual

Digital Verifier, Signature & Certificate

Let's make things safer!

Contents

CONT	TENTS	2
1	INTRODUCTION	3
2	CERTIFICATE MANAGEMENT	4
2.1	Self-signed certificates	5
2.2	CA SIGNED CERTIFICATES	6
3	VIDEO AUTHENTICATION PROCESS	7
3.1	Recording	7
3.2	Export	7
3.3	SIGNATURE & MOVIE TRANSPORTATION	8
3.4	CERTIFICATE TRANSPORTATION & TRUST	9
3	4.1 Extract & Install certificate from signature using Digital Signature Verifier	. 9
3	4.2 Install Certificate by exporting from Video Server	11
3.5	CHECKING SIGNATURE	12
APPE	NDIX A1	4
APPE	NDIX B1	7

1 Introduction

The latest generation of networked systems promises a much easier and faster way of moving video around (e.g. police, court room...), by simply sending it over the Internet. A public network like the Internet is not exactly the safest when talking about transport. However, digital video can be digitally secured and the possibility to trace the video back to its origin is now a reality. This technology is called **digitally signing** the video.

A **digital signature** is a cryptographically encoded text that contains information about the exported movie file that was signed and about the entity that created the signature. Each export file has its own signature.

A **certificate** is again a cryptographically protected text that contains the electronic key with which the owner of the certificate can sign digital documents or content. This certificate is only valuable if it is trusted by the authorities. (See Chapter **2 Certificate Management**)

The following diagram shows how a digital signature is used in the video authentication process. A full step by step explanation can be found in Chapter **3 Video Authentication Process**.



Video Authentication Process

2 Certificate Management

The Certificate Management section allows you to handle your certificates for exported movie signing. This section can be found in the **Video Manager** application under the menu **Settings** \rightarrow **Certificate Management**.

ameras	Alarms	POS	Storage Manager	Single View	Mosaics	Network Video Recor	ders Network S	ettings Certificate Manageme	nt Time Synchronization
					Cert	ificate Manage	ement		
			+		Curi	rent Certificate Inform	nation		
			Subject:		WEBCCT	V F9C878A1-33C5FI	DEF-C3AB5588-5	59CCB45E	
			Issuer:		WEBCCT	V F9C878A1-33C5FI	EF-C3AB5588-5	59CCB45E	
			E-mail:	1	79C878A1	33C5FDEF-C3AB558	8-59CCB45E@1	iospam.com	
			Issued to: W	EBCCTV F9C8	78A1-33C	5FDEF-C3AB5588-59 59CCB45E@n	CCB45E, F9C87 ospam.com	8A1-33C5FDEF-C3AB5588-	
			Issued by: W	WEBCCTV F9C878A1-33C5FDEF-C3AB5588-59CCB45E, F9C878A1-33C5FDEF-C3AB5588- 59CCB45E@nospan.com					
			Days to expire:			36520)		
		1	Created:			Tue Nov 11 09:49:08	UTC+0200 2008		
					(Certificate Manageme	nt		
			Export an encoded	certificate (*.ce	er)			Export	
							E-mail:	webcctv@quadrox.com	
			Generate a new se	lf-signed certific	ate, using	the specified	Location:	Belgium	
			parameters					Generate	
			Import a new certit	icate (* cer. * n	fr)		File on server:		
			import a new terth	icare (.cer, .p	1.1)			Import	
								4	

Certificate Management Screen

The **Current Certificate Information** section consists of general information about the certificate which is currently used by WebCCTV for export movie signing, such as:

- Name of your certificate
- Certificate name of an issuer which signed your certificate
- Email you specified for certificates generating
- Complete information that identifies your certificate (including name, email and location)
- Complete information that identifies certificate of an issuer which signed your certificate (including name, email and location)
- Days left to your certificate expiration
- Date of your certificate generation



Subject/Issuer and **Issued to/Issued by** fields are the same if using a self-signed certificate.

2.1 Self-signed certificates

During the WebCCTV installation a self-signed certificate is created which has nonpersonalized information. It is recommended that you create a new certificate which will include your information as a signer. To do that, follow the steps below:

- 1. Specify your e-mail in the **E-mail** field.
- 2. Specify your location in the **Location** screen.
- 3. Click Generate button.

Your new self-signed certificate has been generated. From now on it is used for signing the export movie files.

To export this certificate for transmitting it to a remote location or other purposes, click the **Export** button and define the location to store.

Self-signed certificate have the following advantages and disadvantages:

Advantages:

- Certificate can be renewed at one's choosing
- Custom information (i.e. location of the recorder and contact email, etc.) can be added which is useful in court
- Certificate doesn't expire
- Certificate is free of charge

Disadvantages:

- Certificate is not verified by 3rd party, so it has limited trust.
- Certificate should be explicitly added to the trusted certificates list on each machine for the verification.



2.2 CA signed certificates

In spite of the self-signed certificates advantages, this approach is not the most secure. To improve your security, Quadrox recommends getting a certificate from a trusted certification authority (CA). There are Certification Authorities (CA) which are explicitly trusted worldwide so Microsoft pre-installed theirs certificates in the Windows Operating System. Hence those certificate authorities are trusted by all 3rd parties which use a Windows Operating System. If you get a certificate signed by the CA, you automatically become a trusted signer in the Windows environment.

To import the CA certificate in the WebCCTV system, follow the steps below:

- 1. Save the certificate on your WebCCTV server.
- 2. Specify the exact path to the certificate in the **File on server** field.
- 3. Click **Import** button.

Exported movie files will now be signed by the imported CA certificate. The main advantage is that you don't need to install it on each machine since this certificate is pre-installed there.

A certificate loses its "trust value" over time, because the longer it is in place, the higher chance it has of being compromised. It is recommended that certificates are renewed regularly and that the old certificate is allowed to expire.

CA certificates have the following advantages and disadvantages:

Advantages:

- Certificate is checked by trusted 3rd party for maximal security
- Certificate doesn't need to be explicitly added to trusted certificates list
- Certificate expires

Disadvantages:

Certificate must be purchased





3 Video Authentication Process

The following diagram shows how a digital signature is used in the video authentication process:



Video Authentication Process

There are six steps in the process:

- Step 1 Recording
- Step 2 Export
- Step 3 Signature & Movie Transportation
- Step 4 + 5 Certificate Transportation & Trust
- Step 6 Checking Signature

3.1 Recording

Video from the camera is recorded in a standard ASF movie file. During export you can choose to keep it in ASF or convert it to WMV. WMV files can be played on every windows based operating system as the WMV codec is installed by default.

3.2 Export

When a relevant piece of video is exported, information about that video (e.g. the timestamp, camera name, recorder information and the user who performed the export) is gathered in a

signature message. This message is encrypted by the certificate, unique to each recorder, to form a digital signature.

WebCCTV supports two formats of digital signature:

- .eml S/MIME standard message like used in digitally signed emails.
- .p7m true PKCS #7 standard signature message. It can be opened by specialized viewers like Cryptigo's P7MViewer (<u>http://www.cryptigo.com</u>).

Quadrox has based all of these systems on the open standard technology to prevent any possibility of security holes or "back doors". All algorithms that are used are well known and widely used cryptographic standards, like MD5, SHA-1 and RSA. They cannot be broken if the key is not known, not even by the people that implemented them. The certificate is standard (X.509, PKSC #12), as is the digital signature format (PKCS #7). Apart from the true signature standard that can be viewed by publicly available specialized viewers, we also provide the signature in a standard email format (S/MIME format) so that it can be viewed by common email clients like Outlook Express. Quadrox uses Microsoft's implementations of these formats and algorithms, which are validated and certified by the National Institute of Standards and Technology (NIST).

3.3 Signature & Movie Transportation

The movie file and the signature are transported to the courtroom. They don't necessarily have to travel together and the channel can be unsafe (e.g. they can be sent over the Internet).

To save the signature for further transportation, follow the steps below:

- Click on the signature you want to save.
- Select the save location in the pop up window and click OK.



Saving Digital Signature Screen



3.4 Certificate Transportation & Trust

The certificate should be trusted by the court. By trusting the validity of a certificate (by manually checking that it is indeed what it claims to be), the court acknowledges explicitly that the certificate belongs to the machine on which the export was created.

The court expresses this trust by explicitly adding it to the list of trusted root certificates. When doing this, the system will ask to manually verify the certificate, e.g. by comparing the thumbprint of the certificate to the thumbprint of the certificate that is present on the recorder. The latter should be retrieved by physically going to the recorder, it should be done by the authorities and a proven track record should be available. Trusting the certificate has to be done only once per recorder (not for every movie) and doesn't have to necessarily happen at the moment of movie verification.



When using CA certificates, the trust in the certificate might come from trusting the CA that delivered the certificate. In that case, this procedure might not be necessary.

A copy of the certificate can be extracted from the signature by using the Digital Signature Verifier (available from the Quadrox website). The certificate can also get to the courtroom in a different way (by exporting it from the recorder) or can already be present because it was extracted from previous movies.

3.4.1 Extract & Install certificate from signature using Digital Signature Verifier

Follow the steps below:

Open the Digital Signature Verifier tool.



Digital Signature Verifier main screen

• Enter the locations of the movie and signature files and click the **Verify** button. If the certificate is not yet trusted, you will see the following screen.



Not trusted certificate warning screen

• Click the **Certificate** button.

ertificate General Details Cer	tification Path	<u>?</u>)				
Certifical	e Information					
This certificate •Ensures the •Proves you •Ensures sof •Protects so •Protects e •Allows data	This certificate is intended to: •Ensures the identity of a remote computer •Proves your identity to a remote computer •Ensures software came from software publisher •Protects software from alteration after publication •Protects e-mail messages •Allows data to be signed with the current time					
Issued to:	QTEST2 D5CB4ED6-C7AC2C61-AC6795EC- A6138FB9	-				
Issued by:	QTEST2 D5CB4ED6-C7AC2C61-AC6795EC- A6138FB9					
Valid from	24/10/2006 to 24/10/2106					
	Install Certificate Issuer Statemen	t				
	ОК					

Certificate Information Screen

- Click **Install Certificate** button and follow further instructions leaving all settings by default. A Security Warning window will appear.
- To make sure that you are installing the exact certificate you need, find the **Thumbprint** line in the Security Warning window and compare it with the thumbprint of the original certificate on the recorder. If the thumbprints match, click **Yes**.

Securi	ty Warning 🛛					
	You are about to install a certificate from a certification authority (CA) claiming to represent:					
	NICK236 9EAC64A8-3C00B177-EFDC7A3C-E0A5215A					
	Windows cannot validate that the certificate is actually from "NICK236 9EAC64A8-3C00B177-EFDC7A3C-E0A5215A". You should confirm its origin by contacting "NICK236 9EAC64A8-3C00B177-EFDC7A3C-E0A5215A". The following number will assist you in this process:					
	Thumbprint (sha1): 712850AA 81C83295 1BD700C2 7852EF05 660E0C0C					
Warning: If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirm thumbprint is a security risk. If you click "Yes" you acknowledge this risk.						
	Do you want to install this certificate?					
	Yes No					

Security Warning Screen

Certificate	? 🛛	? 🛛
General Details Certification Path		1
Show: <all></all>	~	∼
Field	Value 🔼	Value 🔼
Valid from Valid to Subject Public key Subject Alternative Name Thumbprint algorithm	Monday, October 30, 2006 4: Saturday, October 30, 2106 4 herent, test@dobedo.com, NI RFSA (1024 Bits) RFC822 Name=test@dobedo sha1 71 28 50 aa 81 c8 32 95 1b d7	Monday, October 30, 2006 4: Saturday, October 30, 2106 4 herent, test@dobedo.com, NI RSA (1024 Bits) RFC822 Name=test@dobedo sha1 71 28 50 aa 81 c8 32 95 1b d7
Ec	It Properties	dit Properties
	ОК	ОК

Certificate Information Screen

• Once your certificate is installed, repeat the first two points of this chapter. To verify the signature, see Chapter **3.5 Checking Signature**.

3.4.2 Install Certificate by exporting from Video Server

Follow the steps below:

- Open WebCCTV web-client.
- Go to **System-> Certificate Management** section.
- Click **Export** button and define location to store the certificate.

Certificate Management					
Export an encoded certificate (*.cer)		Export			
Generate a new self-signed certificate, using the specified	E-mail:	webcctv@quadrox.com			
	Location:	Belgium			
parameters		Generate			
	File on				
Import a new certificate (*.cer, *.pfx)	server:				
		Import			

Certificate Management Screen

- Transport the exported certificate to the target machine and double click on it. The Certificate Information screen will appear.
- Click **Install Certificate** button and follow further instructions leaving all settings by default. A Security Warning window will appear.
- To make sure that you are installing the exact certificate you need, find the **Thumbprint** line in the Security Warning window and compare it with the thumbprint of the original certificate on the recorder. If the thumbprints match, click **Yes**.



To learn advanced ways to make the certificate explicitly trusted, see Appendix A.

3.5 Checking Signature

Once the certificate is trusted, the signature message can be decoded. Because the certificate is trusted, we know that a) the information in the signature is correct (wasn't changed) and b) the signature was produced on the recorder from which the movie is claimed to have originated. If the signature was forged, the certificate will not decode it. Inside the signature, a hash value links the certificate uniquely to the movie file. By recalculating the hash in the courtroom, we can be sure that a) this signature belongs to this particular movie and b) the movie hasn't changed since the signature was created. If the movie was forged, the hash value would be different and the signature invalid.

These actions are performed automatically by the Digital Signature Verifier tool.

Quadrox Digital Signature Verification	
	Digital Signature Verification
Please select movie file	
D:\WEBCCTVTEST1_CAMERA 4_2006-11-30_11-18	3_2006-11-30_11-26-59_J Browse
Please select signature file	
D:\WEBCCTVTEST1_CAMERA 4_2006-11-30_11-18	3_2006-11-30_11-26-59_/ Browse
About Help	Verify Close

Digital Signature Verifier main screen

- Open the Digital Signature Verifier tool.
- Enter the locations of the movie and signature files and click the **Verify** button.
- If the signature can be decoded and the hash information matches the movie, the movie authenticity is proven and the following information screen will be shown. The displayed information is part of the digital signature and is likewise proven to be authentic.

he signature is trusted. he movie file has not been c	hanged after signing.
Filename	WEBCCTVTEST1_NV5 207 4_2006-11-30_11-18_2006-11-30_11-26-59_rad28283.asf
Start time of the movie	2006-11-30 11:18:00
End time of the movie	2006-11-30 11:26:59
Time of export	2006-11-30 11:35:26
Name of the user that created the	WEBCCTVTEST1\Administrator
Name of the recorder	WEBCCTVTEST1
Name of the camera	NV5 207 4

Trusted signature information screen

• If the signature cannot be trusted because either the signature or the movie was tampered with, the following screen will be shown.



Not trusted signature information screen

The Digital Signature Verifier was created by Quadrox to make your life easier. However, it is not crucial to verifying the digital signature. You are free to manually check the signature, or by a tool of your own choosing.

The tool is released as an open source tool under the BSD license. To make sure that the tool doesn't display false information, feel free to examine the source code and make your own compilation for maximum trust.



To learn how to manually verify the signature, see Appendix B.

Appendix A

Trust certificate explicitly by means of the Outlook Express email client

Follow the steps below:

- 1. Save .eml signature on the target machine.
- 2. Double-click on it to open. You will see the following screen that means your certificate is not trusted on this machine.



MS Outlook Express Untrusted Signature Screen

- 3. Click Edit Trust button.
- 4. In the screen that appears select **Explicitly Trust this Certificate** and follow further prompts.



Signing Digital ID Properties Screen

Trust certificate explicitly by means of the Microsoft Management Console

Follow the steps below:

- 1. Go to **Start->Run** and specify **mmc** command.
- 2. In the window that appears, click **File** in the window menu and select **Add/Remove Snap-in**.
- 3. In the window that appears, click **Add** button.
- 4. In the next appeared window, choose Certificates and click Add button.

Console1				
File Action View Favorites Window Help				
			1	
Console Root				
Console Root	Name			
	There are no items to show in	this view.		
Add/Remove	e Snap-in	YX		
Standalone	Extensions			
Lise this pa	age to add or remove a standalone Snan-in from the console			
Snap-ins a	dded to: 🔄 Console Root 💌			_
		Add Standalone Snap-in		? ×
		Available Standalone Snap-ins:		
		Snap-in	Vendor	
		ActiveX Control	Microsoft Corporation	
		Certificates	Microsoft Corporation	
		Component Services	Microsoft Corporation	
		B Computer Management	Microsoft Corporation	
		Device Manager	Microsoft Corporation	
		Disk Defragmenter	Microsoft Corp, Executi	
		Disk Management	Microsoft and VERITAS	
Descripti	on	Event Viewer	Microsoft Corporation	
			Microsoft Corporation	
· · · · · · · · · · · · · · · · · · ·		Group Policy Ubject Editor	Microsoft Corporation	-
		Description		_
	I Present Allert I	The Certificates snap-in allows you to certificate stores for yourself, a service	browse the contents of the	
Add	Hemove About	contribute stores for yourself, a service	, or a compater.	
	OK C			
			Add Close	

Microsoft Management Console Screen

5. Then select **My User account** item and click **Finish**.

Console1	
File Action View Favorites	Window Help
← → 🖪 🖳 🔗	
Toncolo Root	
Console Root	Name
	There are no Perry to show in this view
	Add/Remove Snap-in
	Standalone Extensions
	Lie bij new is dela una se desetelen Sanz is fere be servele
	dise tris page to add on relinitive a standaurie singer in forme console.
	Snap-ins added to: Console Root
	Certificates snap-in X
	This snap-in will always manage certificates for:
	• My user account
	C Service account
	C Computer account
	Description
I	
	Add Remove About
	OK Ca
	< Back Finish Cancel

Microsoft Management Console Screen

- 6. Close all previously opened windows by pressing Close and OK buttons.
- 7. Finally you will get the list of all installed certificates.

a Console1 - [Console Root\Certificates - Current User\Intermediate Certification Authorities\Certificates]								
🚡 File Action View Favorites Window Help								
Console Root	Issued To 🔺	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status C		
🖻 👹 Certificates - Current User	🖼 GlobalSign Root CA	Root SGC Authority	28/01/2014	1.3.6.1.4.1.311.10	<none></none>			
主 📃 Personal	🖼 GTE CyberTrust Root	Root SGC Authority	23/02/2006	1.3.6.1.4.1.311.10	<none></none>			
Trusted Root Certification Authorities	Microsoft Windows Hardware Com	Microsoft Root Authority	31/12/2002	Code Signing, Windo	<none></none>			
Enterprise Trust	Microsoft Windows Hardware Com	Microsoft Root Authority	31/12/2002	Code Signing, Windo	<none></none>			
Cortificate Devection List	MS SGC Authority	Root SGC Authority	01/01/2010	Server Authenticatio	<none></none>			
	QTEST2 D5CB4ED6-C7AC2C61-AC	QTEST2 D5CB4ED6-C7AC2C61-AC6	24/10/2106	<all></all>	<none></none>			
Active Directory Liser Object	Root Agency	Root Agency	01/01/2040	<a >	<none></none>			
Trusted Publishers	SecureNet CA SGC Root	Root SGC Authority	16/10/2009	1.3.6.1.4.1.311.10	<none></none>			
🗄 💼 Untrusted Certificates	🕮 Thawte Premium Server CA	Root SGC Authority	16/07/2004	1.3.6.1.4.1.311.10	<none></none>			
吏 🚞 Third-Party Root Certification Authoriti	🕮 Thawte Server CA	Root SGC Authority	16/07/2004	1.3.6.1.4.1.311.10	<none></none>			
🗈 🚞 Trusted People	WIN - DATACorp SGC	Root SGC Authority	24/06/2019	1.3.6.1.4.1.311.10	<none></none>			
🖻 💼 Other People	🕮 VeriSign Class 1 CA Individual Sub	Class 1 Public Primary Certification A	13/05/2008	<all></all>	<none></none>			
Certificates	🖼 VeriSign Class 2 CA - Individual Su	Class 2 Public Primary Certification A	07/01/2004	<all></all>	<none></none>			
	🕮 www.verisign.com/CPS Incorp.by	Class 3 Public Primary Certification A	08/01/2004	2.16.840.1.113733	<none></none>			

Microsoft Management Console Screen

- 8. After the certificate installation procedures, which were described above, the certificates are installed to the **Intermediate Certification Authorities** list (when certificate is extracted from the digital signature) or to the **Other People** list (when certificate is installed by exporting it from the recorder). Find your certificate in the corresponding list.
- 9. To make the certificate fully trusted, drag and drop your certificate to the **Trusted Root Certification Authorities** list.

🚡 Console1 - [Console Root\Certificates - Current User\Intermediate Certification Authorities\Certificates]								
🚡 File Action View Favorites Window Help								
Console Root	Issued To 🔺	Issued By	Expiration Date	Intended Purposes	Friendly Name			
🖻 🚳 Certificates - Current User	🖼 GlobalSign Root CA	Root SGC Authority	28/01/2014	1.3.6.1.4.1.311.10	<none></none>			
Personal	🖼 GTE CyberTrust Root	Root SGC Authority	23/02/2006	1.3.6.1.4.1.311.10	<none></none>			
Trusted Root Certification Authorities	Microsoft Windows Hardware Com	Microsoft Root Authority	31/12/2002	Code Signing, Windo	<none></none>			
	🕮 Microsoft Windows Hardware Com	Microsoft Root Authority	31/12/2002	Code Signing, Windo	<none></none>			
Enterprise Trust	MS SGC Authority	Root SGC Authority	01/01/2010	Server Authenticatio	<none></none>			
Certificate Revocation List	QTEST2 D5CB4ED6-C7AC2C61-AC	QTEST2 D5CB4ED6-C7AC2C61-AC6	24/10/2106	<all></all>	<none></none>			
Certificates	Root Agency	Root Agency	01/01/2040	<all></all>	<none></none>			
Active Directory User Object	SecureNet CA SGC Root	Root SGC Authority	16/10/2009	1.3.6.1.4.1.311.10	<none></none>			
🗄 💼 Trusted Publishers	🖼 Thawte Premium Server CA	Root SGC Authority	16/07/2004	1.3.6.1.4.1.311.10	<none></none>			
🕀 💼 Untrusted Certificates	🚟 Thawte Server CA	Root SGC Authority	16/07/2004	1.3.6.1.4.1.311.10	<none></none>			
🗄 💼 Third-Party Root Certification Authoriti	UTN - DATACorp SGC	Root SGC Authority	24/06/2019	1.3.6.1.4.1.311.10	<none></none>			
🗄 💼 Trusted People	VeriSign Class 1 CA Individual Sub	Class 1 Public Primary Certification A	13/05/2008	<all></all>	<none></none>			
🕂 💼 Other People	VeriSign Class 2 CA - Individual Su	Class 2 Public Primary Certification A	07/01/2004	<all></all>	<none></none>			
🗄 💼 Certificate Enrollment Requests	www.verisign.com/CPS Incorp.by	Class 3 Public Primary Certification A	08/01/2004	2.16.840.1.113733	<none></none>			
	1							

Microsoft Management Console Screen

10. After verifying the thumbprint, click Yes in the screen that appears.

iecurity '	Warning 🔀	
	You are about to install a certificate from a certification authority (CA) claiming to represent:	
	QTEST2 D5CB4ED6-C7AC2C61-AC6795EC-A6138FB9	
	Windows cannot validate that the certificate is actually from "QTEST2 D5CB4ED6-C7AC2C61-AC6795EC-A6138FB9". You should confirm its origin by contacting "QTEST2 D5CB4ED6-C7AC2C61-AC6795EC-A6138FB9". The following number will assist you in this process:	
	Thumbprint (sha1): B91DC763 BA4283C4 7FA72B72 C7F49B5C F02C76E6	
	Warning: If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.	
	Do you want to install this certificate?	
	Yes No	

Security Warning Screen

Appendix B

You can manually verify the digital signature by using either the .eml or the .p7m format.

 Signatures in .eml format can be viewed by MS Outlook Express. To do that, double click on the .eml file you just saved, Outlook Express opens the signature and you will see the following screen.

🚔 (No subject)														
Eile Edi	. ⊻iew	Tools M	essage <u>H</u> elp											1
Reply	鹶 Reply All	5 Forward	Print	X Delete	Previous	N ext	M Addresse	85						
From: Date: To: Subject: Security:	invalid@ir Thursday none (No subje Digitally s	nvalid.com , October 2 ect) igned and v	6, 2006 14:08 erified										ļ	2
FileNam HashTyp HashVal TimeStar Server User SystemII Source SourceII MovieSt MovieEr	e ue np)) art d		Q Q Q Q	QTEST2_ MD5 b21f1ad9 2006-10- TEST2 EST2VAd CB4448F: amera 1 3C35776 2006-10-2 2006-10-2	Camera 1_ 26 14:07:2 ministrator F-8CD52I 7-A59A-4 26 11:47:5 26 11:52:5	_2006-1 8753218 25 DEF-6A 467F-92 1 10	0-26_11- 365193ee 425E01-1 FB-5DF(-47-51_ :2 891389 09BCD0	2006-10- 18 DFF0}	26_11-:	52-50_r	adC5899	.asf	*
														-

Digital Signature Screen

 Signatures in .p7m format can be viewed by a p7mViewer or another relevant viewer (<u>http://www.cryptigo.com</u>). To do that, install the viewer and double click on the .p7m file you just saved. The p7mViewer opens the signature and you will see a screen, which is similar to the one that is above.

Being able to open a digital signature file and see the information inside it implies that it can be decoded (and thus was generated) by the certificate. This means that the signature file itself cannot have been tampered with.

The digital signature generated by Quadrox software contains the following information:

- The filename of the signed movie.
- Signed movie hash type and value. Together, filename and hash value indisputably link the signature to the movie file.
- The time at which the video was recorded.
- The name of the recorder where video was recorded and exported.
- The system user that created the movie export.
- The identifier of the recorder, which together with the certificate that was used proves that the movie file was originally recorded on that particular system.
- The name of the camera that recorded the exported footage.
- The identifier of the camera that recorded the exported footage.
- The start time of the exported footage
- The end time of the exported footage.



A hash value or a checksum for a file is a short value, something like a fingerprint of the file. This feature can be useful both for comparing the files and their integrity control.

A hash is a mathematically calculated number that uniquely defines the original information. There are always several information strings that have the same hash as a result, but it is infeasible to find a "second original" based only on the hash. If you change a single bit in the original information, the hash will be different. Popular hashes used by the Quadrox software are MD5 and SHA-1.

The Hash value can be checked by using the special tools which are built upon the MD5 checksum algorithm which is used worldwide for checking the integrity of the files, for example FastSum application (<u>http://www.fastsum.com</u>).

Calculate movie hash value by means of the FastSum application

Follow the steps below:

- 1. Download and install the **FastSum** application by using all the default settings.
- 2. Right-click on the export file and make the selection as shown on the following screen.

\bigcirc	NTCK236_Camera 2_2006-10-30_15-53-02_200 ^V Play Queue-It-Up Add to Playlist Copy to CD or Device	
	▶ FastSum	Create checksums for selected files
	Open With	
	Send To	
	Cut	
	Сору	
	Create Shortcut	
	Delete	
	Rename	
	Properties	

Create Checksum Selection Screen

- 3. Click **F9** button in the FastSum screen that appears to begin the calculation.
- 4. When the checksum is calculated by means of FastSum, compare it with the one from the digital signature.

> FastSum 1.5 [Uni	registered]
File Edit View Run 1	Tools Help
🖻 🔎 📙 •	Circle → Til Register now!
	Choose the files or an entire folder you want to make checksums of Files Folder
	After you save the results you will be able to check the integrity of your files. Press the Save (Ctrl+S) button to save.
	Display the full path in file list
■ Loaded ■ Changed ■ Actual <u>New: 1 (100%)</u>	Name Size Checksum/State Image: Size Checksum/State 4,494 KB F7DD0EDEA50FEEFCF6358804C6738E17
Detecting size: Found 11 Calculating the checksur Calculation complete Processed 1 files in 0 fold Elapsed time: 00:00:00 A	hies in U tolders with total size 4.39 Mb ms ed at 11/2/2006 10:07:29 AM ders with total size 4.39 Mb. ders with total size 4.39 Mb.
	🗁 Selected 4 39 Mb in 1 files 0 folders

FastSum Screen

🚔 (No subject)	
File Edit View Tools Message Help	
Sev Sev Sev Sev Sev Sev Reply Reply All Forward Print Delete Previous Next Addresses	
From: invalid@email.invalid Date: Thursday, November 02, 2006 10:11 AM To: none Subject: (No subject) Security: Digitally signed and verified	8
FileName NICK236_Camera 2_2006-10-30_15-53-02_2006-10-30_15-57- 58_rad61477.asf MD5 HashType MD5 HashValue f7dd0edea50feefcf6358b04c6738e17 TimeStamp 2006-10-30 15:58:51 Server NICK236 User NICK236\Administrator SystemID 5D8DB897-F5237FC0-2B60FC6A-3D0EFC16 Source Camera 2 SourceID (5B29277A-066D-46F2-AE07-8EE126DA30E5) MovieEnd 2006-10-30 15:57:58	
	4

Digital Signature Screen

If the checksums don't correspond with each other, this means the movie file is not valid and has been changed.

Version 4.4 Series

Check hash value of an exported movie file by means of the FastSum application

Follow the steps below:

- 1. Download and install the FastSum application (<u>http://www.fastsum.com</u>).
- 2. Create an empty text file with **.md5** extension.
- 3. Edit the file in the following way:



The string above is an example.

Assuming that

fb21f1ad9a8797c1e875321865193ee2 – is the hash value/checksum, which is taken from the digital signature of the exported movie file you want to validate.

 $\label{eq:QTEST2_Camera 1_2006-10-26_11-47-51_2006-10-26_11-52-50_radC5899.as f-is the name of the exported movie file you want to validate.$

4. Save the edited **.md5** file.

> FastSum 1.5 []

- 5. Put saved .md5 file and export movie file to a one folder.
- 6. Launch **FastSum** application and go to **File -> Verification Wizard**.
- 7. Click Add File in the screen that appears and select .md5 file you created.

e Edit View Run	Tools Help	
a 🔊 🖪 -		juter novel
		Choose the files or an entire folder you want to mak
	(
	Press the Verification Wiza	ard (Ctrl+D) button to load the list.
	Display the full path in file list	
Loaded	Name 🔺	
Changed		
Actual		
		Charlenum Varification Without Ethnonistanad
		You can specify files or an entire folder with checksums you want to verify.
		C:\Exchange\Movie\check.md5
		Add File. Add Filder. Bemove
		Include only following files (Example: a*.*figure*.*):
		Exclude following files (Example: *xis;*:doc)
		<u> </u>

FastSum Application Screen

8. Click Next.

9. If the movie file wasn't changed and the checksum corresponds to the movie file, you will see the following screen:

Checksum Verification Wizard [Unregistered]				
Congratulations				
You have successfully completed the verification of 1 files at the chosen locations.				
Source checksums match actual, files not changed.				
To close this wizard, click Finish.				
< Back Finish (Cancel			

Checksum Verification Wizard Screen

10. If checksum doesn't correspond to the movie file, this means that the movie file is not valid and has been changed. You will see a screen denoting such an error:

Checksum Verification Wizard [Unregistered]X
Oops!	
Unfortunately FastSum was unable to load a integrity cannot be verified. It is required to f selected earlier. To see the errors list click th	ny of the source checksums. The files lave access to the source checksums you le Details button.
🔥 Loading errors:	1 Details
To close this wizard, click Finish.	
Copy Save Report	< Back Finish Cancel

Checksum Verification Wizard Screen