Canon

Digital Signatures

- Would you like to prevent unauthorized alteration of PDF documents?
- Are you looking to track and identify where scanned documents originated?
- Are you looking for a feature that will increase device management options and allow greater control over network devices?
- Are you looking to ensure the authenticity of documents?
- Are you looking to prevent security leaks?

Solution

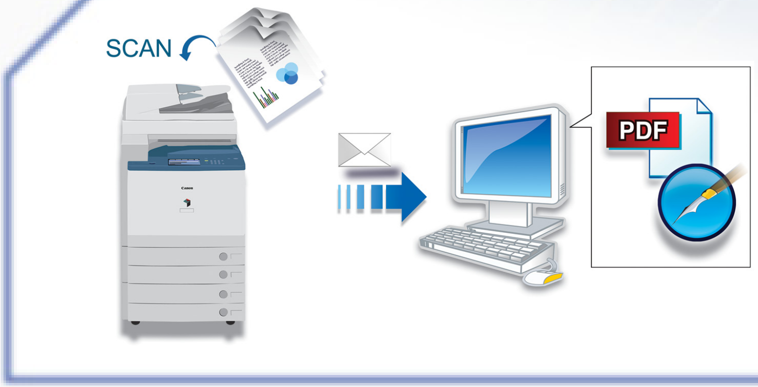
imageRUNNER® Digital Signature Function

The Digital Signature function enables you to add a Device Signature and/or User Signature to a PDF document to help track and prevent security problems, such as impersonation and unauthorized alteration of documents.

Device Signature and User Signature are the two types of digital signatures:

1. **Device Signature attaches the digital signature of the device to the PDF file. Device Signature shows from which device the PDF was sent, time, date, and if the document has been altered.**
2. **User Signature enables a user to attach a digital signature of the user to the PDF file. User Signature includes the original sender's name, e-mail address, time, date, and if the document has been altered.**

It's important to remember that if you need to add a Digital User Signature to a PDF, it's necessary to log-in to the machine using the SDL or SSO log-in service.



NOTE: The features discussed may not be available for all imageRUNNER devices; optional equipment may be required. Check with your local Authorized Canon Dealer for more information.

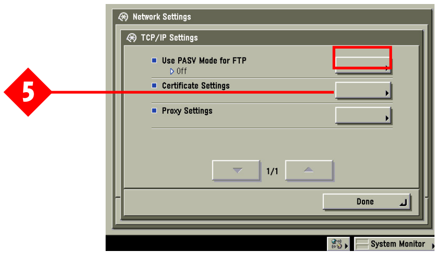
How Do You Do It?

Digital Device Signature PDF

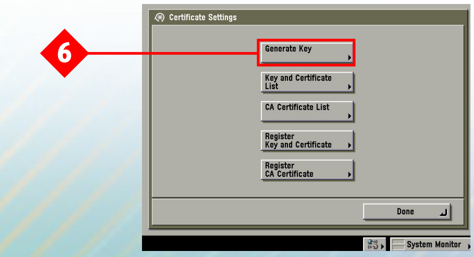
Generating a Key Pair and Device Signature Certificate

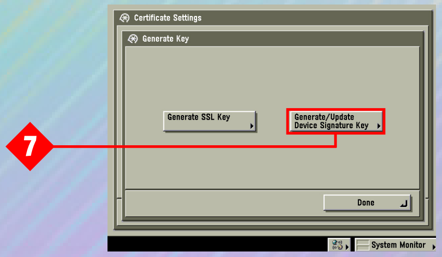
(initial set up only)

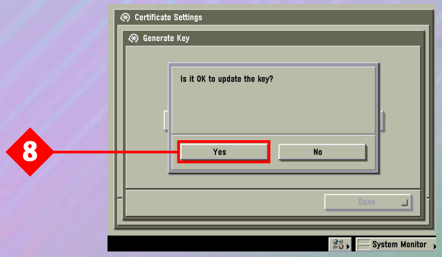
1. Press [**Additional Functions**] on the key pad.
2. On the LCD panel, select [**System Settings**].
3. Select [**Network Settings**].
4. Select [**TCP/IP**].
5. Select [**Certificate Settings**].
6. Select [**Generate Key**].
7. Select [**Generate/Update Device Signature Key**].
8. Select [**Yes**] to generate/update a key.
9. When finished, select [**Done**] on the status screen to return to the Certificate Settings screen.



Use PASV Mode for FTP ▷ Off





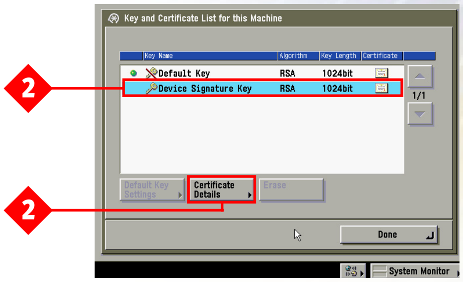


Is it OK to update the key?

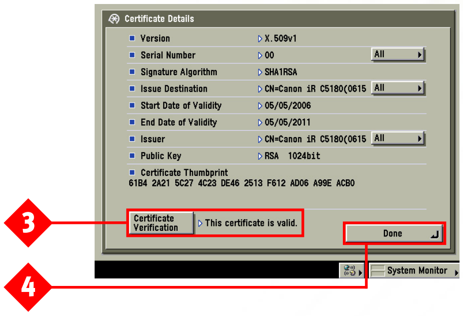
Confirming a Key Pair and Device Signature Certificate

(initial set up only)

1. On the Certificate Settings screen, select [**Key and Certificate List for this Machine**].
2. Only one key pair can be registered and is named ‘Device Signature Key.’ Select [**Device Signature Key**] and press [**Certificate Details**].
3. Press [**Certificate Verification**] to confirm its validity. If so, a message appears “This certificate is valid.” Certificates expire five (5) years after the key is generated/updated.
4. Press [**Done**] on each screen to return to the Send screen.



Key Name	Algorithm	Key Length	Certificate
Default Key	RSA	1024bit	
Device Signature Key	RSA	1024bit	

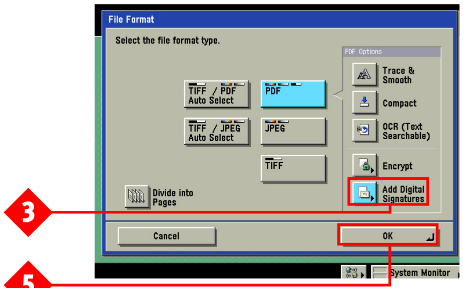


- Version ▷ X.509v1
- Serial Number ▷ 00
- Signature Algorithm ▷ SHA1RSA
- Issue Destination ▷ CN=Canon iR C5180(0615
- Start Date of Validity ▷ 05/05/2006
- End Date of Validity ▷ 05/05/2011
- Issuer ▷ CN=Canon iR C5180(0615
- Public Key ▷ RSA 1024bit
- Certificate Thumbprint 61B4 2A21 5C27 4C23 DE46 2513 F612 AD06 A99E ACB0

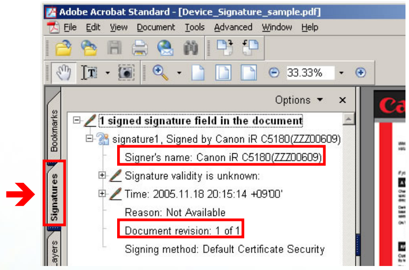
▷ This certificate is valid.

Adding a Device Signature to a PDF File

1. Place your originals in the document feeder or on the glass.
2. Select [**File Format**] to access the Device Signature feature.
3. Select [**Add Digital Signatures**].
4. Select [**Add Device Signature**] and press [**OK**].
5. You can add other PDF options to this document, and then select [**OK**].
6. Enter or select a destination from the Address Book, then press the [**Start**] button to send the document.



Select the file format type.

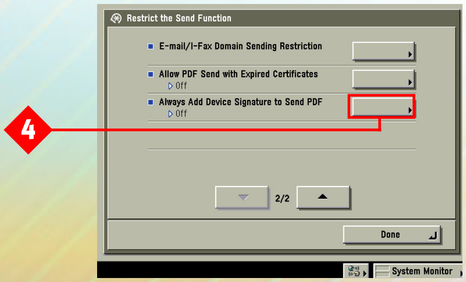


1 signed signature field in the document
signature1, Signed by Canon iR C5180(ZZZ00609)
Signer's name: Canon iR C5180(ZZZ00609)
Signature validity is unknown:
Time: 2005.11.18 20:15:14 +09'00'
Reason: Not Available
Document revision: 1 of 1
Signing method: Default Certificate Security

Name and serial number of device displays under Signature tab in PDF file.

Setting Always Add a Device Signature to Send PDF

1. Press [**Additional Functions**] on the keypad.
2. Select [**System Settings**].
3. Select [**Restrict the Send Function**].
4. Select [**Always Add Device Signature to Send PDF**] and press [**On**].
5. Select [**OK**], then [**Done**] until returned to initial screen.


4
Restrict the Send Function
E-mail/I-Fax Domain Sending Restriction
2/2
Done
System Monitor

- Allow PDF Send with Expired Certificates ▷ Off
- Always Add Device Signature to Send PDF ▷ Off

Demo Scenarios

Legal

The law firm of May, Fan, and Stein specializes in class action law suits and has multiple offices throughout the country working on the same cases. By utilizing a Digital User Signature PDF, satellite offices can scan all case documents and securely send to their lead attorney. By using Digital User Signature PDF, the lead attorney can identify the original sender and determine from which attorney the documents originated. This helps ensure that all documents received are valid and genuine.

Financial Services

Metropolis Bank is promoting its home equity loans because of a new low introductory rate. Loan Officers scan the applications into the imageRUNNER devices at each branch office and send PDF documents to the processing department. Each application is stamped with a Digital Device Signature for added security and proper identification. The back-office processing department uses the Digital Device Signature feature to identify each branch that originated the loan. The Device Signature feature assists the processing department by ensuring that the loan application is being sent from its branch network. This helps protect customer information and enhances internal data security.

Healthcare

Tepper Health Services (THS) has a large medical records office that frequently needs to send portions of medical records to authorized parties. To comply with HIPAA Privacy and Security* rules and help provide accountability and documentation, THS has deployed imageRUNNER devices with the Digital User Signature feature in its medical records office. When a user is logged into the device using SDL then scans and sends any medical record, the sending user's identification is automatically attached to the PDF file and logged into the imageRUNNER devices log of sent documents. This facilitates compliance with privacy laws by providing a record of when documents are sent as well as by whom.

**Canon U.S.A. does not provide legal counsel or compliance consultancy, including without limitation, HIPAA. Each customer should consult with his/her legal counsel to determine the advisability of this solution as it relates to regulatory compliance.*

NOTE: The scenarios listed above are fictitious and are for illustrative purposes only.

Digital Signature Solution

Benefits

- Helps ensure the authenticity of the document.
- Shows where the received PDF documents originated.
- Creates log of user-identifying information.
- Provides each user with his/her own digital credentials for sending and signing documents.
- Adds time and date of when document was scanned originally.
- Verifies whether a document has been altered.

FAQ

Q: How do I get these security features on my Color imageRUNNER device?

A: Digital Device Signature mode is part of the Universal Send PDF Security Feature Set, while Digital User Signature is an optional kit. (Device Signature is optional on the compatible “Base” imageRUNNER devices, and standard on the compatible “i” Series imageRUNNER devices.)

Q: How is a Digital Device Signature created?

A: Device Signature mode uses the device signature certificate and key pair inside the machine to add a digital signature to the document.

Q: Do Digital Device Signatures expire?

A: Device signatures have a finite lifetime and expire five (5) years after the signature key pair is generated or updated.

Q: How is a Digital User Signature installed on an imageRUNNER device?

A: This type of signature requires the optional Digital User Signature PDF Kit. It’s necessary to install a key pair and user certificate in the machine from a computer. The key pair and user certificate can be confirmed using the device.

Q: How are Digital User Signatures obtained?

A: Digital credentials and public key infrastructures (PKIs) can be obtained in two ways. They can be issued from an independent certificate authority (such as VeriSign™) or a company’s internal Windows® 2000/2003 Server with an IIS Module. It’s also necessary to install it on the device through Remote UI.

Q: Do users have to log into the imageRUNNER device to employ Digital User Signature PDF?

A: Yes. Each user must log into the imageRUNNER device using the standard SDL or SSO log-in methods. If the user has not been authenticated, the person won’t be able to apply his/her Digital User Signature to the PDF.

Q: How can I tell who signed a document?

A: Using the Document Signature Tab in Adobe® Acrobat® will show which user signed the document.

Q: How many individual Digital User Signatures can be installed on an imageRUNNER device?

A: Up to 100 Digital User Signatures may be installed on an imageRUNNER device supporting this feature, making it an ideal solution for large departments or workgroups.

Canon
imageANYWARE

1-800-OK-CANON
www.usa.canon.com

Canon U.S.A., Inc.
One Canon Plaza
Lake Success, NY 11042

Device functions subject to change without notice.