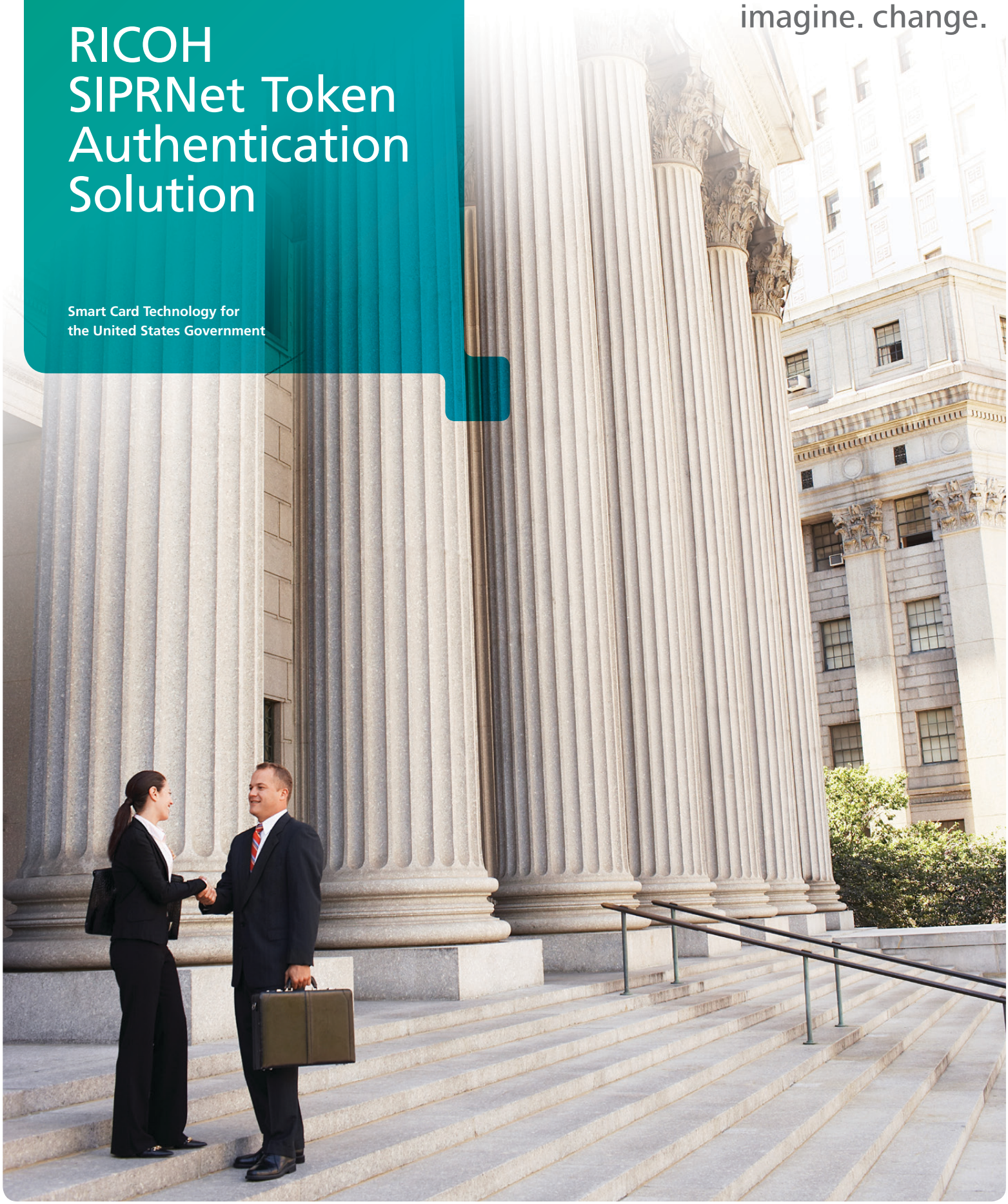
RICOH
imagine. change.

RICOH SIPRNet Token Authentication Solution

Smart Card Technology for the United States Government



RICOH SIPRNet Token Authentication Solution

Protect Critical Information from Unauthorized Users

Hundreds of thousands of federal employees, contractors and even vendors may have access to the Secret Internet Protocol Router Network (SIPRNet), a medium-security computer network for sharing information classified "Secret" or below. Even more people want access — and not all with the best intentions in mind. Use the RICOH® SIPRNet Token Authentication Solution to help protect against unauthorized access to the SIPRNet, a U.S. federal government internal version of the Internet. With this easy-to-use, but hard-to-penetrate card authentication system, users insert their government-issued identity card at a card reader connected to the Ricoh MFP. Once authenticated, the user can access key MFP capabilities to capture, distribute, store and retrieve confidential data through the SIPRNet network.

Perform everyday tasks with less risk

You can work faster when you're not looking over your shoulder. With the RICOH SIPRNet Token Authentication Solution, you simply insert the government-issued identity card you already use to access buildings and rooms into an attached card reader, type in your authentication PIN and start performing document management tasks. Users can print, copy, fax or scan documents, including sending information through scan-to-email or scan-to-folder, and even access document server functions right from the MFP, knowing that the information is secure. For added security, administrators can assign an authentication passcode up to 16 digits.

Identify who and what to protect

There's a wide range of roles in the federal government. It's up to decision makers like you to determine how much information is needed for each one. You can use the RICOH SIPRNet Token Authentication Solution to specify what can be done with that information, too. Each user's ID card is embedded with specific credentials that are shared with a database of authenticated users. You can decide if a user has access to all MFP functionality or only selected features. For example, you can restrict scan-to-email for specific users or for an entire workgroup to minimize information leaks.

Sign up for more secure encryption

Have confidence that your information will reach its intended audience — and only that audience. The RICOH SIPRNet Token Authentication Solution includes Secure/Multipurpose Internet Mail Extension (S/MIME) technology, so authorized users can digitally sign and encrypt emails. Only approved recipients can decrypt the message, so you know the information should remain secure until it reaches its proper destination. And, because it's signed, the person will know exactly who sent it. You can combine this feature with global (LDAP) address book search capabilities to give authorized users a faster way to capture and distribute higher priority documents.

Meet the highest government security standards

No organization has more clearance levels and sophisticated strategies for ensuring the right people have the right information than the federal government. That's why it's critical that you meet only the most stringent government standards for protecting information. The RICOH SIPRNet Token Authentication Solution is FIPS 140-2 validated for scan-to-email. It meets requirements of the Homeland Security Presidential Directive-12 (HSPD-12). Plus, it's integrated with 90Meter authentication technology, so your information benefits from some of the most powerful security features available.

Take advantage of multiple authentication methods

The U.S. government is a vast organization, with many agencies in locations around the world. We're prepared to help protect information for users wherever they are. Choose from a wide range of authentication methods to meet your specific needs, including:

- OCSP Server
  - Primary
  - Secondary
  - Proxy
- Active Directory
  - Kerberos Realm (Microsoft Windows® Server 2008-2016)
- Certificate Revocation List (CRL)

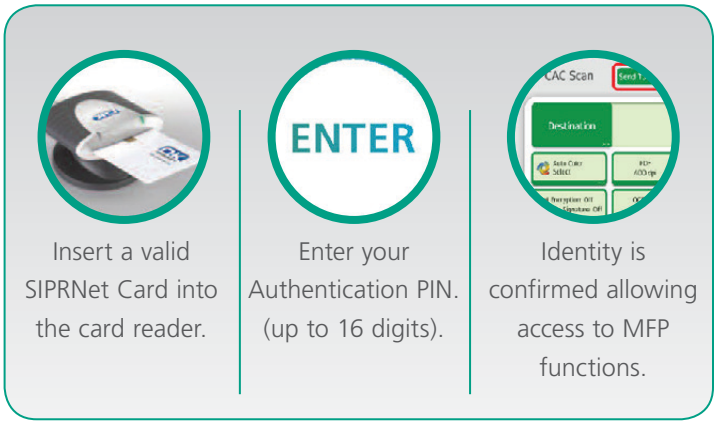
Specifications

SIPRNet-compatible Ricoh MFPs

Select Java Version 10.x, 11.x and 12.x MFPs

Required MFP Features/Options	Printer/Scanner Kit USB Host Interface Java VM SD Card
Ricoh-tested SIPRNet Readers	SCM Microsystems: SCR3310 v2
Required Customer-supplied Items	SIPRNet Smart Card OCSP Server URL(s) OCSP Server Certificate(s) Root CA Certificate(s) Sub CA Certificate(s)

Note: The OCSP Server URL(s) and Security Certificate(s) can be obtained from the on-site Security Administrator.



Insert a valid SIPRNet Card into the card reader.

Enter your Authentication PIN. (up to 16 digits).

Identity is confirmed allowing access to MFP functions.

RICOH imagine. change.

www.ricoh-usa.com

Ricoh Americas Corporation, 70 Valley Stream Parkway, Malvern, PA 19355 1-800-63-RICOH