FIPS Java API provider and non-FIPS provider

Classic List Threaded

Rhuberg,Anthony

Jun 05, 2018; 2:01pm **FIPS Java API provider and non-FIPS provider**

15 posts

We have an application deployed within Tomcat and that application is uses Apache CXF which has a dependency on bcprov-jdk1

Referring to: https://www.bouncycastle.org/fips-java/BCFipsIn100.pdf: "The provider jar itself has no external dependencies, bu JVM as the regular Bouncy Castle provider. The classes in the two jar files do not get along".

We are integrating FIPS Java API provider into another application WAR. We have not encountered an issues yet, but wanted to expected if two applications use different Bouncy Castle Java implementations within the same JVM.

Thanks,Tony

CONFIDENTIALITY NOTICE This message and any included attachments are from Cerner Corporation and are intended only for the addressee. The information contained in this messa public information under international, federal, or state securities laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be promptly delete this message and notify the sender of the delivery error by e-mail or you may call Cerner's corporate offices in Kansas City, Missouri, U.S.A at (+1) (816)221-1024.

Matti Aarnio

Jun 05, 2018; 2:33pm **Re: FIPS Java API provider and non-FIPS provider**

32 posts

Hi Tony,

The detail that affects more than "in same JVM" is "are they in same class loader?"

WARs are loaded into separate class loader chains.
WAR1 gets loader chain: CL1, CLroot.
WAR2 gets loader chain: CL2, CLroot.

If neither BCFIPS nor BCPROV are in CLroot, and instead in separate WARs,
then the libraries will not see each other, and no collision happens.

The "CLroot" is server/lib/ in current Tomcats.
The "CLn" is webapps/warname/WEB-INF/lib/

Best Regards, Matti

On 05.06.2018 21:01, Rhuberg,Anthony wrote:

> We have an application deployed within Tomcat and that application is uses Apache CXF which has a dependency on bcpro
>
> Referring to: https://www.bouncycastle.org/fips-java/BCFipsIn100.pdf: "The provider jar itself has no external dependenci the same JVM as the regular Bouncy Castle provider. The classes in the two jar files do not get along".
>
> We are integrating FIPS Java API provider into another application WAR. We have not encountered an issues yet, but want errors are expected if two applications use different Bouncy Castle Java implementations within the same JVM.
>
> Thanks,Tony

Rhuberg,Anthony

Jun 05, 2018; 2:40pm **RE: FIPS Java API provider and non-FIPS provider**

15 posts

Thanks. Makes sense.

From: Matti Aarnio [mailto:[hidden email]]
Sent: Tuesday, June 05, 2018 2:33 PM
To: Rhuberg,Anthony <[hidden email]>; [hidden email]
Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider

Hi Tony,

The detail that affects more than "in same JVM" is "are they in same class loader?"

WARs are loaded into separate class loader chains.
WAR1 gets loader chain: CL1, CLroot.
WAR2 gets loader chain: CL2, CLroot.

If neither BCFIPS nor BCPROV are in CLroot, and instead in separate WARs,
then the libraries will not see each other, and no collision happens.

The "CLroot" is server/lib/ in current Tomcats.
The "CLn" is webapps/warname/WEB-INF/lib/

Best Regards, Matti

On 05.06.2018 21:01, Rhuberg,Anthony wrote:

> We have an application deployed within Tomcat and that application is uses Apache CXF which has a dependency on bcpro
>
> Referring to: https://www.bouncycastle.org/fips-java/BCFipsIn100.pdf: “The provider jar itself has no external dependenci the same JVM as the regular Bouncy Castle provider. The classes in the two jar files do not get along”.
>
> We are integrating FIPS Java API provider into another application WAR. We have not encountered an issues yet, but want errors are expected if two applications use different Bouncy Castle Java implementations within the same JVM.
>
> Thanks,Tony

CONFIDENTIALITY NOTICE This message and any included attachments are from Cerner Corporation and are intended only for the addressee. The information contained in this messa public information under international, federal, or state securities laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be promptly delete this message and notify the sender of the delivery error by e-mail or you may call Cerner's corporate offices in Kansas City, Missouri, U.S.A at (+1) (816)221-1024.

Rhuberg,Anthony

Jun 19, 2018; 3:04pm **RE: FIPS Java API provider and non-FIPS provider**

15 posts

In reply to this post by Matti Aarnio

Just a follow up from my previous question…

We have a configuration with a Tomcat Valve which uses opensaml (with a dependency on xmlsec -> bcprov-jdk15on). These cl loader (call it CLroot).

We just started using bc-fips-1.0.1.jar for digital signatures in a web application. That jar is part of the war (call it CL1).

Based on this configuration, we expected to observe some conflict when executing the pathways for the Tomcat Valve and web a

The applications are “working”, but worry that there is some unseen or potential problem that we have just not encountered.

Any thoughts? Do you have an examples of how a collision (between the 2 jars bcprov-jdk15on - bc-fips-1.0.1.jar) would be ma typical errors when there is a conflict?

Thanks,

Tony

From: Matti Aarnio [mailto:[hidden email]]
Sent: Tuesday, June 05, 2018 2:33 PM
To: Rhuberg,Anthony <[hidden email]>; [hidden email]
Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider

Hi Tony,

The detail that affects more than "in same JVM" is "are they in same class loader?"

WARs are loaded into separate class loader chains.
WAR1 gets loader chain: CL1, CLroot.
WAR2 gets loader chain: CL2, CLroot.

If neither BCFIPS nor BCPROV are in CLroot, and instead in separate WARs,
then the libraries will not see each other, and no collision happens.

The "CLroot" is server/lib/ in current Tomcats.
The "CLn" is webapps/warname/WEB-INF/lib/

Best Regards, Matti

On 05.06.2018 21:01, Rhuberg,Anthony wrote:

> We have an application deployed within Tomcat and that application is uses Apache CXF which has a dependency on bcpro
>
> Referring to: https://www.bouncycastle.org/fips-java/BCFipsIn100.pdf: "The provider jar itself has no external dependenci the same JVM as the regular Bouncy Castle provider. The classes in the two jar files do not get along".
>
> We are integrating FIPS Java API provider into another application WAR. We have not encountered an issues yet, but want errors are expected if two applications use different Bouncy Castle Java implementations within the same JVM.
>
> Thanks,Tony

CONFIDENTIALITY NOTICE This message and any included attachments are from Cerner Corporation and are intended only for the addressee. The information contained in this messa public information under international, federal, or state securities laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be promptly delete this message and notify the sender of the delivery error by e-mail or you may call Cerner's corporate offices in Kansas City, Missouri, U.S.A at (+1) (816)221-1024.

David Hook-3

Jun 19, 2018; 6:17pm **Re: FIPS Java API provider and non-FIPS provider**

253 posts

The high risk element is the JCE - it depends how it gets loaded and if both things make use of the respective providers. Often tl system class loader and in that case there can be only one.

If bcprov isn't loaded in the system class loader and/or bc-fips is able to satisfy the dependency anyway, you will probably be ok

General the problems you see if it is an issue don't make sense. You'll get issues with undefined methods, class not found, missi get class cast exceptions where it seems impossible as well.

If you want to ask the OpenSAML guys to talk to us we would be happy to help them update.

Regards,

David

On 20/06/18 05:04, Rhuberg,Anthony wrote:

> Just a follow up from my previous question…
>
> We have a configuration with a Tomcat Valve which uses opensaml (with a dependency on xmlsec -> bcprov-jdk15on). Th
> root class loader (call it CLroot).
>
> We just started using bc-fips-1.0.1.jar for digital signatures in a web application. That jar is part of the war (call it CL1).
>
> Based on this configuration, we expected to observe some conflict when executing the pathways for the Tomcat Valve and
>
> The applications are "working", but worry that there is some unseen or potential problem that we have just not encountere

... [show rest of quote]

Rhuberg,Anthony

Jun 20, 2018; 9:52am **RE: FIPS Java API provider and non-FIPS provider**

15 posts

Is there a way to identify the bc-fips dependencies (pom.xml or other list) so that we can package them within our application w
Tomcat will resolve all dependencies if found by the WAR class loader and therefore not resolve down to the system class loader

Thanks,

Tony

From: David Hook [mailto:[hidden email]]
Sent: Tuesday, June 19, 2018 6:18 PM
To: Rhuberg,Anthony <[hidden email]>; Matti Aarnio <[hidden email]>; [hidden email]
Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider

The high risk element is the JCE - it depends how it gets loaded and if both things make use of the respective providers. Often tl
system class loader and in that case there can be only one.

If bcprov isn't loaded in the system class loader and/or bc-fips is able to satisfy the dependency anyway, you will probably be ok

General the problems you see if it is an issue don't make sense. You'll get issues with undefined methods, class not found, missi
get class cast exceptions where it seems impossible as well.

If you want to ask the OpenSAML guys to talk to us we would be happy to help them update.

Regards,

David

On 20/06/18 05:04, Rhuberg,Anthony wrote:

> Just a follow up from my previous question…
>
> We have a configuration with a Tomcat Valve which uses opensaml (with a dependency on xmlsec -> bcprov-jdk15on). Th
> root class loader (call it CLroot).
>
> We just started using bc-fips-1.0.1.jar for digital signatures in a web application. That jar is part of the war (call it CL1).
>
> Based on this configuration, we expected to observe some conflict when executing the pathways for the Tomcat Valve and
>
> The applications are "working", but worry that there is some unseen or potential problem that we have just not encountere

… [show rest of quote]

Rhuberg,Anthony

Jun 20, 2018; 10:31am **RE: FIPS Java API provider and non-FIPS provider**

15 posts

Nevermind. I also noticed that we include apache-cxf within our application WAR. It has a dependency on org.apache.cxf:cxf-rt-
dependency on opensaml; we changed are packaging to exclude opensaml from the WAR since it was included on the system pa
resolve this conflict other than changing opensaml (and resolving any impacts on those third-parties that depend on it).

From: Rhuberg,Anthony
Sent: Wednesday, June 20, 2018 9:53 AM
To: 'David Hook' <[hidden email]>; Matti Aarnio <[hidden email]>; [hidden email]
Subject: RE: [dev-crypto] FIPS Java API provider and non-FIPS provider

Is there a way to identify the bc-fips dependencies (pom.xml or other list) so that we can package them within our application w
Tomcat will resolve all dependencies if found by the WAR class loader and therefore not resolve down to the system class loader

Thanks,

Tony

From: David Hook [[hidden email]]
Sent: Tuesday, June 19, 2018 6:18 PM
To: Rhuberg,Anthony <[hidden email]>; Matti Aarnio <[hidden email]>; [hidden email]
Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider

The high risk element is the JCE - it depends how it gets loaded and if both things make use of the respective providers. Often tl
system class loader and in that case there can be only one.

If bcprov isn't loaded in the system class loader and/or bc-fips is able to satisfy the dependency anyway, you will probably be ok

General the problems you see if it is an issue don't make sense. You'll get issues with undefined methods, class not found, missi
get class cast exceptions where it seems impossible as well.

If you want to ask the OpenSAML guys to talk to us we would be happy to help them update.

Regards,

David

On 20/06/18 05:04, Rhuberg,Anthony wrote:

> Just a follow up from my previous question…
>
> We have a configuration with a Tomcat Valve which uses opensaml (with a dependency on xmlsec -> bcprov-jdk15on). Th
> root class loader (call it CLroot).
>
> We just started using bc-fips-1.0.1.jar for digital signatures in a web application. That jar is part of the war (call it CL1).

> Based on this configuration, we expected to observe some conflict when executing the pathways for the Tomcat Valve and
>
> The applications are “working”, but worry that there is some unseen or potential problem that we have just not encountere

... [show rest of quote]

Rhuberg,Anthony

Jun 20, 2018; 2:58pm **RE: FIPS Java API provider and non-FIPS provider**

15 posts

In reply to this post by David Hook-3

Hi again,

I am trying to understand the conflict further and am not really familiar with JCA/JCE.

If both JCE providers ‵bcprov´and ‵bcfips’ are loaded into the same class loader, I do not understand the conflict if they both hav implementation classes. If I request a Signature.getinstance(“SHA256withRSA”, “BCFIPS”), would I not get the bcfips implement instance?

Can multiple JCE providers be deployed within an application and the application decide which implementation to use without co providers to coexist.

Is this conflict a BC conflict only? I am asking because if we selected another JCE provider (to get around this issue) and still hav would we still have a similar conflict between another provider and bcprov?

Thanks again,

Tony

From: David Hook [mailto:[hidden email]]
Sent: Tuesday, June 19, 2018 6:18 PM
To: Rhuberg,Anthony <[hidden email]>; Matti Aarnio <[hidden email]>; [hidden email]
Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider

The high risk element is the JCE - it depends how it gets loaded and if both things make use of the respective providers. Often tl system class loader and in that case there can be only one.

If bcprov isn't loaded in the system class loader and/or bc-fips is able to satisfy the dependency anyway, you will probably be ok

General the problems you see if it is an issue don't make sense. You'll get issues with undefined methods, class not found, missi get class cast exceptions where it seems impossible as well.

If you want to ask the OpenSAML guys to talk to us we would be happy to help them update.

Regards,

David

On 20/06/18 05:04, Rhuberg,Anthony wrote:

> Just a follow up from my previous question…
>
> We have a configuration with a Tomcat Valve which uses opensaml (with a dependency on xmlsec -> bcprov-jdk15on). Th
> root class loader (call it CLroot).
>
> We just started using bc-fips-1.0.1.jar for digital signatures in a web application. That jar is part of the war (call it CL1).
>
> Based on this configuration, we expected to observe some conflict when executing the pathways for the Tomcat Valve and
>
> The applications are "working", but worry that there is some unseen or potential problem that we have just not encountere

... [show rest of quote]

Eckenfels. Bernd

Jun 20, 2018; 3:18pm **RE: FIPS Java API provider and non-FIPS provider**

142 posts

The problem is that BC and BcFiPS have conflicting implementation classes. There is some logic to that (be a plugin replacement
than it helps. Maybe it would be a option to offer a FIPS jar with distinct namespace for those cases.

--
http://www.seeburger.com

From: Rhuberg,Anthony [[hidden email]]
Sent: Wednesday, June 20, 2018 20:58
To: David Hook; Matti Aarnio; [hidden email]
Subject: RE: [dev-crypto] FIPS Java API provider and non-FIPS provider

Hi again,

I am trying to understand the conflict further and am not really familiar with JCA/JCE.

If both JCE providers 'bcprov´and 'bcfips' are loaded into the same class loader, I do not understand the conflict if they both hav
implementation classes. If I request a Signature.getinstance("SHA256withRSA", "BCFIPS"), would I not get the bcfips implement
instance?

Can multiple JCE providers be deployed within an application and the application decide which implementation to use without co
providers to coexist.

Is this conflict a BC conflict only? I am asking because if we selected another JCE provider (to get around this issue) and still hav
would we still have a similar conflict between another provider and bcprov?

Thanks again,
Tony

From: David Hook [mailto:[hidden email]]
Sent: Tuesday, June 19, 2018 6:18 PM
To: Rhuberg,Anthony <[hidden email]>; Matti Aarnio <[hidden email]>; [hidden email]
Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider

The high risk element is the JCE - it depends how it gets loaded and if both things make use of the respective providers. Often t
system class loader and in that case there can be only one.

If bcprov isn't loaded in the system class loader and/or bc-fips is able to satisfy the dependency anyway, you will probably be ok

General the problems you see if it is an issue don't make sense. You'll get issues with undefined methods, class not found, missi
get class cast exceptions where it seems impossible as well.

If you want to ask the OpenSAML guys to talk to us we would be happy to help them update.

Regards,

David

On 20/06/18 05:04, Rhuberg,Anthony wrote:
Just a follow up from my previous question…

We have a configuration with a Tomcat Valve which uses opensaml (with a dependency on xmlsec -> bcprov-jdk15on). These cl
loader (call it CLroot).
We just started using bc-fips-1.0.1.jar for digital signatures in a web application. That jar is part of the war (call it CL1).

Based on this configuration, we expected to observe some conflict when executing the pathways for the Tomcat Valve and web a

The applications are “working”, but worry that there is some unseen or potential problem that we have just not encountered.

Any thoughts? Do you have an examples of how a collision (between the 2 jars bcprov-jdk15on - bc-fips-1.0.1.jar) would be ma
typical errors when there is a conflict?

Thanks,
Tony

From: Matti Aarnio [mailto:[hidden email]]
Sent: Tuesday, June 05, 2018 2:33 PM
To: Rhuberg,Anthony <[hidden email]><mailto:[hidden email]>; [hidden email]<mailto:[hidden email]>
Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider

Hi Tony,

The detail that affects more than "in same JVM" is "are they in same class loader?"

WARs are loaded into separate class loader chains.
WAR1 gets loader chain: CL1, CLroot.
WAR2 gets loader chain: CL2, CLroot.

If neither BCFIPS nor BCPROV are in CLroot, and instead in separate WARs,
then the libraries will not see each other, and no collision happens.

The "CLroot" is server/lib/ in current Tomcats.
The "CLn" is webapps/warname/WEB-INF/lib/

Best Regards, Matti

On 05.06.2018 21:01, Rhuberg,Anthony wrote:

We have an application deployed within Tomcat and that application is uses Apache CXF which has a dependency on bcprov-jdk1

Referring to: https://www.bouncycastle.org/fips-java/BCFipsIn100.pdf<https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.bouncycastle.org%2Ffips-java%2FBCFipsIn100.pdf&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7Ce60fa34500a84aeb1a7a08d5cb12c856%7
“The provider jar itself has no external dependencies, but it cannot be used in the same JVM as the regular Bouncy Castle provid
do not get along”.

We are integrating FIPS Java API provider into another application WAR. We have not encountered an issues yet, but wanted to
expected if two applications use different Bouncy Castle Java implementations within the same JVM.

Thanks,Tony

CONFIDENTIALITY NOTICE This message and any included attachments are from Cerner Corporation and are intended only for t
contained in this message is confidential and may constitute inside or non-public information under international, federal, or stat
forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be unlawful. If you are not th
delete this message and notify the sender of the delivery error by e-mail or you may call Cerner's corporate offices in Kansas Cit
(816)221-1024.

SEEBURGER AG   Vorstand/SEEBURGER Executive Board:
Sitz der Gesellschaft/Registered Office: Axel Haas, Michael Kleeberg, Friedemann Heinz, Dr. Martin Kuntz, Matthias Fe
Edisonstr. 1
D-75015 Bretten   Vorsitzende des Aufsichtsrats/Chairperson of the SEEBURGER Supervisory Board:
Tel.: 07252 / 96 - 0   Prof. Dr. Simone Zeuchner
Fax: 07252 / 96 - 2222
Internet: http://www.seeburger.de   Registergericht/Commercial Register:
e-mail: [hidden email]   HRB 240708 Mannheim

Dieses E-Mail ist nur für den Empfänger bestimmt, an den es gerichtet ist und kann vertrauliches bzw. unter das Berufsgeheimni
Jegliche darin enthaltene Ansicht oder Meinungsäußerung ist die des Autors und stellt nicht notwendigerweise die Ansicht oder M
Sind Sie nicht der Empfänger, so haben Sie diese E-Mail irrtümlich erhalten und jegliche Verwendung, Veröffentlichung, Weiterle
Druck dieser E-Mail ist strengstens untersagt. Weder die SEEBURGER AG noch der Absender (Eckenfels. Bernd) übernehmen die
Verantwortung, die E-Mail und deren Anhänge auf Viren zu prüfen.

This email is intended only for the recipient(s) to whom it is addressed. This email may contain confidential material that may be
Any fact or opinion contained, or expression of the material herein, does not necessarily reflect that of SEEBURGER AG. If you ar
received this email in error, any use, publication or distribution including forwarding, copying or printing is strictly prohibited. Ne
sender (Eckenfels. Bernd) accept liability for viruses; it is your responsibility to check this email and its attachments for viruses.

Rhuberg,Anthony

Jun 20, 2018; 3:49pm **RE: FIPS Java API provider and non-FIPS provider**

15 posts

Thanks for the clarification. I found at least one class in the same package with a different implementation in bc-fips than bcprov
workflow, but it explains the conflict.

-----Original Message-----
From: Eckenfels. Bernd [mailto:[hidden email]]
Sent: Wednesday, June 20, 2018 3:19 PM
To: [hidden email]
Subject: RE: [dev-crypto] FIPS Java API provider and non-FIPS provider

The problem is that BC and BcFiPS have conflicting implementation classes. There is some logic to that (be a plugin replacement
than it helps. Maybe it would be a option to offer a FIPS jar with distinct namespace for those cases.

--
https://na01.safelinks.protection.outlook.com/?
url=http%3A%2F%2Fwww.seeburger.com&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7C0480b4cbfcff443e0de708
____
From: Rhuberg,Anthony [[hidden email]]
Sent: Wednesday, June 20, 2018 20:58
To: David Hook; Matti Aarnio; [hidden email]
Subject: RE: [dev-crypto] FIPS Java API provider and non-FIPS provider

Hi again,

I am trying to understand the conflict further and am not really familiar with JCA/JCE.

If both JCE providers 'bcprov´and 'bcfips' are loaded into the same class loader, I do not understand the conflict if they both hav
implementation classes. If I request a Signature.getinstance("SHA256withRSA", "BCFIPS"), would I not get the bcfips implement
instance?

Can multiple JCE providers be deployed within an application and the application decide which implementation to use without co
providers to coexist.

Is this conflict a BC conflict only? I am asking because if we selected another JCE provider (to get around this issue) and still hav
would we still have a similar conflict between another provider and bcprov?

Thanks again,
Tony

From: David Hook [mailto:[hidden email]]
Sent: Tuesday, June 19, 2018 6:18 PM
To: Rhuberg,Anthony <[hidden email]>; Matti Aarnio <[hidden email]>; [hidden email]
Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider

The high risk element is the JCE - it depends how it gets loaded and if both things make use of the respective providers. Often th
system class loader and in that case there can be only one.

If bcprov isn't loaded in the system class loader and/or bc-fips is able to satisfy the dependency anyway, you will probably be ok

General the problems you see if it is an issue don't make sense. You'll get issues with undefined methods, class not found, missi
get class cast exceptions where it seems impossible as well.

If you want to ask the OpenSAML guys to talk to us we would be happy to help them update.

Regards,

David

On 20/06/18 05:04, Rhuberg,Anthony wrote:
Just a follow up from my previous question.

We have a configuration with a Tomcat Valve which uses opensaml (with a dependency on xmlsec -> bcprov-jdk15on). These cla
loader (call it CLroot).
We just started using bc-fips-1.0.1.jar for digital signatures in a web application. That jar is part of the war (call it CL1).

Based on this configuration, we expected to observe some conflict when executing the pathways for the Tomcat Valve and web a

The applications are "working", but worry that there is some unseen or potential problem that we have just not encountered.

Any thoughts? Do you have an examples of how a collision (between the 2 jars bcprov-jdk15on - bc-fips-1.0.1.jar) would be ma
typical errors when there is a conflict?

Thanks,
Tony

From: Matti Aarnio [mailto:[hidden email]]

Sent: Tuesday, June 05, 2018 2:33 PM
To: Rhuberg,Anthony <[hidden email]><mailto:[hidden email]>; [hidden email]<mailto:[hidden email]>
Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider

Hi Tony,

The detail that affects more than "in same JVM" is "are they in same class loader?"

WARs are loaded into separate class loader chains.
WAR1 gets loader chain: CL1, CLroot.
WAR2 gets loader chain: CL2, CLroot.

If neither BCFIPS nor BCPROV are in CLroot, and instead in separate WARs, then the libraries will not see each other, and no col

The "CLroot" is server/lib/ in current Tomcats.
The "CLn" is webapps/warname/WEB-INF/lib/

Best Regards, Matti

On 05.06.2018 21:01, Rhuberg,Anthony wrote:

We have an application deployed within Tomcat and that application is uses Apache CXF which has a dependency on bcprov-jdk1

Referring to: https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.bouncycastle.org%2Ffips-java%2FBCFipsIn100.pdf&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7C0480b4cbfcff443e0de708d5d6e2ba56%7Cf
url=https%3A%2F%2Fwww.bouncycastle.org%2Ffips-java%2FBCFipsIn100.pdf&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7Ce60fa34500a84aeb1a7a08d5cb12c856%7C
"The provider jar itself has no external dependencies, but it cannot be used in the same JVM as the regular Bouncy Castle provid
do not get along".

We are integrating FIPS Java API provider into another application WAR. We have not encountered an issues yet, but wanted to
expected if two applications use different Bouncy Castle Java implementations within the same JVM.

Thanks,Tony

CONFIDENTIALITY NOTICE This message and any included attachments are from Cerner Corporation and are intended only for t
contained in this message is confidential and may constitute inside or non-public information under international, federal, or stat
forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be unlawful. If you are not th
delete this message and notify the sender of the delivery error by e-mail or you may call Cerner's corporate offices in Kansas Cit
(816)221-1024.

SEEBURGER AG Vorstand/SEEBURGER Executive Board:
Sitz der Gesellschaft/Registered Office: Axel Haas, Michael Kleeberg, Friedemann Heinz, Dr. Martin Kuntz, Matthias Fe
Edisonstr. 1
D-75015 Bretten Vorsitzende des Aufsichtsrats/Chairperson of the SEEBURGER Supervisory Board:
Tel.: 07252 / 96 - 0 Prof. Dr. Simone Zeuchner
Fax: 07252 / 96 - 2222
Internet: https://na01.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.seeburger.de&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7C0480b4cbfcff443e0de708d5
Registergericht/Commercial Register:
e-mail: [hidden email] HRB 240708 Mannheim

Dieses E-Mail ist nur für den Empfänger bestimmt, an den es gerichtet ist und kann vertrauliches bzw. unter das Berufsgeheimni
Jegliche darin enthaltene Ansicht oder Meinungsäußerung ist die des Autors und stellt nicht notwendigerweise die Ansicht oder M
Sind Sie nicht der Empfänger, so haben Sie diese E-Mail irrtümlich erhalten und jegliche Verwendung, Veröffentlichung, Weiterle
Druck dieser E-Mail ist strengstens untersagt. Weder die SEEBURGER AG noch der Absender (Eckenfels. Bernd) übernehmen die
Verantwortung, die E-Mail und deren Anhänge auf Viren zu prüfen.

This email is intended only for the recipient(s) to whom it is addressed. This email may contain confidential material that may be
Any fact or opinion contained, or expression of the material herein, does not necessarily reflect that of SEEBURGER AG. If you ar
received this email in error, any use, publication or distribution including forwarding, copying or printing is strictly prohibited. Ne
sender (Eckenfels. Bernd) accept liability for viruses; it is your responsibility to check this email and its attachments for viruses.

Rhuberg,Anthony

Jun 20, 2018; 4:33pm **Re: FIPS Java API provider and non-FIPS provider**

15 posts

Is it possible or an option to change the package names of bouncy castle fips implementation? Changing the name would create
not conflict with any other providers.

From: Rhuberg,Anthony <[hidden email]>
Sent: Wednesday, June 20, 2018 3:49:52 PM
To: [hidden email]; [hidden email]
Subject: RE: [dev-crypto] FIPS Java API provider and non-FIPS provider

Thanks for the clarification. I found at least one class in the same package with a different implementation in bc-fips t
affects our workflow, but it explains the conflict.

-----Original Message-----
From: Eckenfels. Bernd [[hidden email]]
Sent: Wednesday, June 20, 2018 3:19 PM
To: [hidden email]
Subject: RE: [dev-crypto] FIPS Java API provider and non-FIPS provider

The problem is that BC and BcFiPS have conflicting implementation classes. There is some logic to that (be a plugin re
to hurt more than it helps. Maybe it would be a option to offer a FIPS jar with distinct namespace for those cases.

--
https://na01.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.seeburger.com&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7C0480b4cbfcff44

____
From: Rhuberg,Anthony [[hidden email]]
Sent: Wednesday, June 20, 2018 20:58
To: David Hook; Matti Aarnio; [hidden email]
Subject: RE: [dev-crypto] FIPS Java API provider and non-FIPS provider

Hi again,

I am trying to understand the conflict further and am not really familiar with JCA/JCE.

If both JCE providers 'bcprov´and 'bcfips' are loaded into the same class loader, I do not understand the conflict if the
names and implementation classes. If I request a Signature.getinstance("SHA256withRSA", "BCFIPS"), would I not ge
NOT the bcprov instance?

Can multiple JCE providers be deployed within an application and the application decide which implementation to use
expecting providers to coexist.

Is this conflict a BC conflict only? I am asking because if we selected another JCE provider (to get around this issue) a
class loader, would we still have a similar conflict between another provider and bcprov?

Thanks again,
Tony

From: David Hook [[hidden email]]
Sent: Tuesday, June 19, 2018 6:18 PM
To: Rhuberg,Anthony <[hidden email]>; Matti Aarnio <[hidden email]>; [hidden email]
Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider

The high risk element is the JCE - it depends how it gets loaded and if both things make use of the respective provide
up in the system class loader and in that case there can be only one.

If bcprov isn't loaded in the system class loader and/or bc-fips is able to satisfy the dependency anyway, you will prob

General the problems you see if it is an issue don't make sense. You'll get issues with undefined methods, class not fo
cases you will get class cast exceptions where it seems impossible as well.

If you want to ask the OpenSAML guys to talk to us we would be happy to help them update.

Regards,

David

On 20/06/18 05:04, Rhuberg,Anthony wrote:
Just a follow up from my previous question.

We have a configuration with a Tomcat Valve which uses opensaml (with a dependency on xmlsec -> bcprov-jdk15on
root class loader (call it CLroot).
We just started using bc-fips-1.0.1.jar for digital signatures in a web application. That jar is part of the war (call it CL

Based on this configuration, we expected to observe some conflict when executing the pathways for the Tomcat Valve

The applications are "working", but worry that there is some unseen or potential problem that we have just not encou

Any thoughts? Do you have an examples of how a collision (between the 2 jars bcprov-jdk15on - bc-fips-1.0.1.jar) w
examples of typical errors when there is a conflict?

Thanks,
Tony

From: Matti Aarnio [[hidden email]]
Sent: Tuesday, June 05, 2018 2:33 PM
To: Rhuberg,Anthony <[hidden email]><mailto:[hidden email]>; [hidden email]<mailto:[hidden email]>
Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider

Hi Tony,

The detail that affects more than "in same JVM" is "are they in same class loader?"

WARs are loaded into separate class loader chains.
WAR1 gets loader chain: CL1, CLroot.
WAR2 gets loader chain: CL2, CLroot.

If neither BCFIPS nor BCPROV are in CLroot, and instead in separate WARs, then the libraries will not see each other,

The "CLroot" is server/lib/ in current Tomcats.
The "CLn" is webapps/warname/WEB-INF/lib/

Best Regards, Matti

On 05.06.2018 21:01, Rhuberg,Anthony wrote:

We have an application deployed within Tomcat and that application is uses Apache CXF which has a dependency on b

Referring to: https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.bouncycastle.org%2Ffips-java%2FBCFipsIn100.pdf&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7C0480b4cbfcff443e0de708d5d6e2
url=https%3A%2F%2Fwww.bouncycastle.org%2Ffips-java%2FBCFipsIn100.pdf&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7Ce60fa34500a84aeb1a7a08d5cb1
"The provider jar itself has no external dependencies, but it cannot be used in the same JVM as the regular Bouncy Ca
two jar files do not get along".

We are integrating FIPS Java API provider into another application WAR. We have not encountered an issues yet, but
errors are expected if two applications use different Bouncy Castle Java implementations within the same JVM.

Thanks,Tony

CONFIDENTIALITY NOTICE This message and any included attachments are from Cerner Corporation and are intendec
information contained in this message is confidential and may constitute inside or non-public information under intern
securities laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibite
are not the addressee, please promptly delete this message and notify the sender of the delivery error by e-mail or yc
offices in Kansas City, Missouri, U.S.A at (+1) (816)221-1024.

SEEBURGER AG Vorstand/SEEBURGER Executive Board:
Sitz der Gesellschaft/Registered Office: Axel Haas, Michael Kleeberg, Friedemann Heinz, Dr. Martin Kuntz, M
Edisonstr. 1
D-75015 Bretten Vorsitzende des Aufsichtsrats/Chairperson of the SEEBURGER Supervisory Board:
Tel.: 07252 / 96 - 0 Prof. Dr. Simone Zeuchner
Fax: 07252 / 96 - 2222
Internet: https://na01.safelinks.protection.outlook.com/?
url=http%3A%2F%2Fwww.seeburger.de&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7C0480b4cbfcff443
Registergericht/Commercial Register:
e-mail: [hidden email] HRB 240708 Mannheim

Dieses E-Mail ist nur für den Empfänger bestimmt, an den es gerichtet ist und kann vertrauliches bzw. unter das Beru
enthalten. Jegliche darin enthaltene Ansicht oder Meinungsäußerung ist die des Autors und stellt nicht notwendigerwe
SEEBURGER AG dar. Sind Sie nicht der Empfänger, so haben Sie diese E-Mail irrtümlich erhalten und jegliche Verwenc
Weiterleitung, Abschrift oder jeglicher Druck dieser E-Mail ist strengstens untersagt. Weder die SEEBURGER AG noch c
übernehmen die Haftung für Viren; es obliegt Ihrer Verantwortung, die E-Mail und deren Anhänge auf Viren zu prüfen

This email is intended only for the recipient(s) to whom it is addressed. This email may contain confidential material t
professional secrecy. Any fact or opinion contained, or expression of the material herein, does not necessarily reflect t
are not the addressee or if you have received this email in error, any use, publication or distribution including forward
strictly prohibited. Neither SEEBURGER AG, nor the sender (Eckenfels. Bernd) accept liability for viruses; it is your res

and its attachments for viruses.

David Hook-3

Jun 21, 2018; 4:22am **Re: FIPS Java API provider and non-FIPS provider**

253 posts

The FIPS package can't be changed. You could do a "spongycastle" on the original Bouncy Castle ones.

The FIPS library doesn't have an implementation of the low-level BC library. From a FIPS point of view the low-level API breaks r
probably a couple they did not consider.

Providers can certainly co-exist, but package name clashes (at least in the system class loader) are right out.

Regards,

David

On 21/06/18 06:33, Rhuberg,Anthony wrote:

> Is it possible or an option to change the package names of bouncy castle fips implementation? Changing the name would c
> that would not conflict with any other providers.
>
> **From:** Rhuberg,Anthony [hidden email]
> **Sent:** Wednesday, June 20, 2018 3:49:52 PM
> **To:** [hidden email]; [hidden email]
> **Subject:** RE: [dev-crypto] FIPS Java API provider and non-FIPS provider
>
> Thanks for the clarification. I found at least one class in the same package with a different implementation in bc-
> sure that affects our workflow, but it explains the conflict.
>
> -----Original Message-----
> From: Eckenfels. Bernd [[hidden email]]
> Sent: Wednesday, June 20, 2018 3:19 PM

... [show rest of quote]

Rhuberg,Anthony

Jun 22, 2018; 9:48am **RE: FIPS Java API provider and non-FIPS provider**

15 posts

Hi,

I appreciate your help trying to resolve this conflict.

Also, forgive my persistence.

We require a FIPS compliant/validated crypto module. I do not think "spongycastle-like" is an alternative. We are including both
parties already require use of the non-FIPS compliant jar (not something we can readily change). If I understand this correctly, t
with common classes in either the bcfips and bcprov jars that contain the same classes with different implementations (that are
jars are never intended to be integrated with the same application, I suppose I understand that limitation, but that probably mal
jar when other third parties (out of our/your control) use the non-fips version.

Can the FIPS package not be changed because that would require it to be revalidated (by CMVP) ? What would be the effort nece
bcprov to coexist? Maybe we could discuss this offline.

Respectfully,

Tony

From: David Hook [mailto:[hidden email]]
Sent: Thursday, June 21, 2018 4:22 AM

To: Rhuberg,Anthony <[hidden email]>; [hidden email]; [hidden email]
Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider

The FIPS package can't be changed. You could do a "spongycastle" on the original Bouncy Castle ones.

The FIPS library doesn't have an implementation of the low-level BC library. From a FIPS point of view the low-level API breaks r
probably a couple they did not consider.

Providers can certainly co-exist, but package name clashes (at least in the system class loader) are right out.

Regards,

David

On 21/06/18 06:33, Rhuberg,Anthony wrote:

> Is it possible or an option to change the package names of bouncy castle fips implementation? Changing the name would c
> that would not conflict with any other providers.
>
> ---
>
> **From:** Rhuberg,Anthony [hidden email]
> **Sent:** Wednesday, June 20, 2018 3:49:52 PM
> **To:** [hidden email]; [hidden email]
> **Subject:** RE: [dev-crypto] FIPS Java API provider and non-FIPS provider
>
> Thanks for the clarification. I found at least one class in the same package with a different implementation in bc-fips than I
> affects our workflow, but it explains the conflict.

... [show rest of quote]

David Hook-3

Jun 22, 2018; 6:12pm **Re: FIPS Java API provider and non-FIPS provider**

253 posts

Hi,

Yes, the FIPS package cannot be changed as it would require revalidation, although that's really a financial, not a technical restra

There is a bit more to it though - the jars can't be used in the same application as it would make it almost impossible to be sure
FIPS compliant. You would only need a 3rd party library to be calling the BC lightweight API to use a non-certified function and it
co-exist, it just won't work like that.

I'm happy to discuss this further off list, I'd just need a bit more background on what you're trying to do.

Regards,

David

On 22/06/18 23:48, Rhuberg,Anthony wrote:

> Hi,
>
> I appreciate your help trying to resolve this conflict.
>
> Also, forgive my persistence.
>
> We require a FIPS compliant/validated crypto module. I do not think "spongycastle-like" is an alternative. We are including
> our third parties already require use of the non-FIPS compliant jar (not something we can readily change). If I understand
> seems to be an issue with common classes in either the bcfips and bcprov jars that contain the same classes with different
> causing the name clashes). If these jars are never intended to be integrated with the same application, I suppose I unders
> probably makes it impossible to use the bcfips jar when other third parties (out of our/your control) use the non-fips versio

... [show rest of quote]

Rhuberg,Anthony Jun 26, 2018; 5:22pm **RE: FIPS Java API provider and non-FIPS provider**

15 posts

Hi,

In our web application deployment within Tomcat, the bcprov.jar is loaded by both the common class loader and the web applica
party dependencies). Our web application has a requirement to digitally sign a prescription (which is the reason for the FIPS com
application does not need to be FIPS compliant, just one of many workflows.

Is the following a reasonable alternative to avoid the package clash?

1. Stop packaging bc-fips-1.0.1.jar in our web application (WAR) – the bcprov will exist in the common class loader and web
2. bc-fips-1.0.1.jar on the filesystem C:\fipsmodule
3. Create a URLClassLoader and load bc-fips-1.0.1.jar
4. Load the BouncyCastleFipsProvider class at runtime

```
    public static final Provider getProvider() throws … {

        List<URL> urls = new ArrayList();

        for (File f : new File("C:/fipsmodule").listFiles()) {

            urls.add(f.~~toURL~~());

        }

        URLClassLoader classLoader = new URLClassLoader(urls.stream().toArray(URL[]::new), null);

        Provider provider = (Provider) classLoader

                .loadClass("org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider").newInstance();

        return provider;

    }


    public byte[] sign(KeyStore keystore, String data) throws …{

       Signature signature = Signature.getInstance("SHA256withRSA", getProvider());

        signature.initSign((PrivateKey) keystore.getKey(getKeyAlias(), getKeystorePassword()));

        signature.update(data.getBytes());

        return signature.sign();

    }
```

Thanks

From: David Hook [mailto:[hidden email]]
Sent: Friday, June 22, 2018 6:13 PM
To: Rhuberg,Anthony <[hidden email]>; [hidden email]; [hidden email]
Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider

Hi,

Yes, the FIPS package cannot be changed as it would require revalidation, although that's really a financial, not a technical restr

There is a bit more to it though - the jars can't be used in the same application as it would make it almost impossible to be sure
FIPS compliant. You would only need a 3rd party library to be calling the BC lightweight API to use a non-certified function and i
co-exist, it just won't work like that.

I'm happy to discuss this further off list, I'd just need a bit more background on what you're trying to do.

Regards,

David

On 22/06/18 23:48, Rhuberg,Anthony wrote:

Hi,

I appreciate your help trying to resolve this conflict.

Also, forgive my persistence.

We require a FIPS compliant/validated crypto module. I do not think "spongycastle-like" is an alternative. We are including our third parties already require use of the non-FIPS compliant jar (not something we can readily change). If I understand seems to be an issue with common classes in either the bcfips and bcprov jars that contain the same classes with different causing the name clashes). If these jars are never intended to be integrated with the same application, I suppose I unders probably makes it impossible to use the bcfips jar when other third parties (out of our/your control) use the non-fips versic

... [show rest of quote]

Eckenfels. Bernd

Jun 26, 2018; 6:07pm **RE: FIPS Java API provider and non-FIPS provider**

142 posts

In your case I would put all the sensitive logic to sign and handle keys in a dedicated VM and use it via remote call. That not onl your keys much better, with the added benefit of beeing fully compliant with all requirements the FIPS provider has to be actuall limit admin access to the key store that way.

Class loader tricks do not really work well for registered providers since they use the classloader from where they are registered.

Bernd
--
http://www.seeburger.com

From: Rhuberg,Anthony [[hidden email]]
Sent: Tuesday, June 26, 2018 23:22
To: David Hook; Eckenfels. Bernd; [hidden email]
Subject: RE: [dev-crypto] FIPS Java API provider and non-FIPS provider

Hi,

In our web application deployment within Tomcat, the bcprov.jar is loaded by both the common class loader and the web applica party dependencies). Our web application has a requirement to digitally sign a prescription (which is the reason for the FIPS com application does not need to be FIPS compliant, just one of many workflows.

Is the following a reasonable alternative to avoid the package clash?

1. Stop packaging bc-fips-1.0.1.jar in our web application (WAR) – the bcprov will exist in the common class loader and web a
2. bc-fips-1.0.1.jar on the filesystem C:\fipsmodule
3. Create a URLClassLoader and load bc-fips-1.0.1.jar
4. Load the BouncyCastleFipsProvider class at runtime

```
public static final Provider getProvider() throws … {
    List<URL> urls = new ArrayList();
    for (File f : new File("C:/fipsmodule").listFiles()) {
        urls.add(f.toURL());
    }
    URLClassLoader classLoader = new URLClassLoader(urls.stream().toArray(URL[]::new), null);
    Provider provider = (Provider) classLoader
            .loadClass("org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider").newInstance();
    return provider;
}

public byte[] sign(KeyStore keystore, String data) throws …{
   Signature signature = Signature.getInstance("SHA256withRSA", getProvider());
    signature.initSign((PrivateKey) keystore.getKey(getKeyAlias(), getKeystorePassword()));
    signature.update(data.getBytes());
    return signature.sign();
}
```

Thanks

From: David Hook [mailto:[hidden email]]
Sent: Friday, June 22, 2018 6:13 PM
To: Rhuberg,Anthony <[hidden email]>; [hidden email]; [hidden email]
Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider

Hi,

Yes, the FIPS package cannot be changed as it would require revalidation, although that's really a financial, not a technical restr

There is a bit more to it though - the jars can't be used in the same application as it would make it almost impossible to be sure
FIPS compliant. You would only need a 3rd party library to be calling the BC lightweight API to use a non-certified function and it
co-exist, it just won't work like that.

I'm happy to discuss this further off list, I'd just need a bit more background on what you're trying to do.

Regards,

David

On 22/06/18 23:48, Rhuberg,Anthony wrote:
Hi,

I appreciate your help trying to resolve this conflict.

Also, forgive my persistence.

We require a FIPS compliant/validated crypto module. I do not think "spongycastle-like" is an alternative. We are including both
parties already require use of the non-FIPS compliant jar (not something we can readily change). If I understand this correctly, t
with common classes in either the bcfips and bcprov jars that contain the same classes with different implementations (that are
jars are never intended to be integrated with the same application, I suppose I understand that limitation, but that probably mal
jar when other third parties (out of our/your control) use the non-fips version.

Can the FIPS package not be changed because that would require it to be revalidated (by CMVP) ? What would be the effort nece
bcprov to coexist? Maybe we could discuss this offline.

Respectfully,
Tony

From: David Hook [mailto:[hidden email]]
Sent: Thursday, June 21, 2018 4:22 AM
To: Rhuberg,Anthony <[hidden email]><mailto:[hidden email]>; [hidden email]<mailto:[hidden email]>; [hidden email]<mailt
Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider

The FIPS package can't be changed. You could do a "spongycastle" on the original Bouncy Castle ones.

The FIPS library doesn't have an implementation of the low-level BC library. From a FIPS point of view the low-level API breaks r
probably a couple they did not consider.

Providers can certainly co-exist, but package name clashes (at least in the system class loader) are right out.

Regards,

David

On 21/06/18 06:33, Rhuberg,Anthony wrote:
Is it possible or an option to change the package names of bouncy castle fips implementation? Changing the name would create
not conflict with any other providers.

____
From: Rhuberg,Anthony <[hidden email]><mailto:[hidden email]>
Sent: Wednesday, June 20, 2018 3:49:52 PM
To: [hidden email]<mailto:[hidden email]>; [hidden email]<mailto:[hidden email]>
Subject: RE: [dev-crypto] FIPS Java API provider and non-FIPS provider

Thanks for the clarification. I found at least one class in the same package with a different implementation in bc-fips than bcprov
workflow, but it explains the conflict.

-----Original Message-----
From: Eckenfels. Bernd [mailto:[hidden email]]
Sent: Wednesday, June 20, 2018 3:19 PM
To: [hidden email]<mailto:[hidden email]>
Subject: RE: [dev-crypto] FIPS Java API provider and non-FIPS provider

The problem is that BC and BcFiPS have conflicting implementation classes. There is some logic to that (be a plugin replacement
than it helps. Maybe it would be a option to offer a FIPS jar with distinct namespace for those cases.

--
https://na01.safelinks.protection.outlook.com/?
url=http%3A%2F%2Fwww.seeburger.com&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7C0480b4cbfcff443e0de708
____
From: Rhuberg,Anthony [[hidden email]<mailto:[hidden email]>]
Sent: Wednesday, June 20, 2018 20:58
To: David Hook; Matti Aarnio; [hidden email]<mailto:[hidden email]>
Subject: RE: [dev-crypto] FIPS Java API provider and non-FIPS provider

Hi again,

I am trying to understand the conflict further and am not really familiar with JCA/JCE.

If both JCE providers 'bcprov´and 'bcfips' are loaded into the same class loader, I do not understand the conflict if they both hav
implementation classes. If I request a Signature.getinstance("SHA256withRSA", "BCFIPS"), would I not get the bcfips implement
instance?

Can multiple JCE providers be deployed within an application and the application decide which implementation to use without co
providers to coexist.

Is this conflict a BC conflict only? I am asking because if we selected another JCE provider (to get around this issue) and still hav
would we still have a similar conflict between another provider and bcprov?

Thanks again,
Tony

From: David Hook [mailto:[hidden email]]
Sent: Tuesday, June 19, 2018 6:18 PM
To: Rhuberg,Anthony <[hidden email]><mailto:[hidden email]>; Matti Aarnio <[hidden email]><mailto:[hidden email]>; [hidd
Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider

The high risk element is the JCE - it depends how it gets loaded and if both things make use of the respective providers. Often t
system class loader and in that case there can be only one.

If bcprov isn't loaded in the system class loader and/or bc-fips is able to satisfy the dependency anyway, you will probably be ok

General the problems you see if it is an issue don't make sense. You'll get issues with undefined methods, class not found, missi
get class cast exceptions where it seems impossible as well.

If you want to ask the OpenSAML guys to talk to us we would be happy to help them update.

Regards,

David

On 20/06/18 05:04, Rhuberg,Anthony wrote:
Just a follow up from my previous question.

We have a configuration with a Tomcat Valve which uses opensaml (with a dependency on xmlsec -> bcprov-jdk15on). These cl
loader (call it CLroot).
We just started using bc-fips-1.0.1.jar for digital signatures in a web application. That jar is part of the war (call it CL1).

Based on this configuration, we expected to observe some conflict when executing the pathways for the Tomcat Valve and web a

The applications are "working", but worry that there is some unseen or potential problem that we have just not encountered.

Any thoughts? Do you have an examples of how a collision (between the 2 jars bcprov-jdk15on - bc-fips-1.0.1.jar) would be ma
typical errors when there is a conflict?

Thanks,
Tony

From: Matti Aarnio [mailto:[hidden email]]
Sent: Tuesday, June 05, 2018 2:33 PM
To: Rhuberg,Anthony <[hidden email]><mailto:[hidden email]><mailto:[hidden email]><mailto:[hidden email]>; [hidden ema
[hidden email]><mailto:[hidden email]>
Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider

Hi Tony,

The detail that affects more than "in same JVM" is "are they in same class loader?"

WARs are loaded into separate class loader chains.
WAR1 gets loader chain: CL1, CLroot.
WAR2 gets loader chain: CL2, CLroot.

If neither BCFIPS nor BCPROV are in CLroot, and instead in separate WARs, then the libraries will not see each other, and no col

The "CLroot" is server/lib/ in current Tomcats.
The "CLn" is webapps/warname/WEB-INF/lib/

Best Regards, Matti

On 05.06.2018 21:01, Rhuberg,Anthony wrote:

We have an application deployed within Tomcat and that application is uses Apache CXF which has a dependency on bcprov-jdk1

Referring to: https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.bouncycastle.org%2Ffips-java%2FBCFipsIn100.pdf&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7C0480b4cbfcff443e0de708d5d6e2ba56%7Cf
url=https%3A%2F%2Fwww.bouncycastle.org%2Ffips-java%2FBCFipsIn100.pdf&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7Ce60fa34500a84aeb1a7a08d5cb12c856%7C
<https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.bouncycastle.org%2Ffips-java%2FBCFipsIn100.pdf&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7C0480b4cbfcff443e0de708d5d6e2ba56%7Cf
url=https%3A%2F%2Fwww.bouncycastle.org%2Ffips-java%2FBCFipsIn100.pdf&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7Ce60fa34500a84aeb1a7a08d5cb12c856%7C
"The provider jar itself has no external dependencies, but it cannot be used in the same JVM as the regular Bouncy Castle provid
do not get along".

We are integrating FIPS Java API provider into another application WAR. We have not encountered an issues yet, but wanted to
expected if two applications use different Bouncy Castle Java implementations within the same JVM.

Thanks,Tony

CONFIDENTIALITY NOTICE This message and any included attachments are from Cerner Corporation and are intended only for t
contained in this message is confidential and may constitute inside or non-public information under international, federal, or stat
forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be unlawful. If you are not th
delete this message and notify the sender of the delivery error by e-mail or you may call Cerner's corporate offices in Kansas Cit
(816)221-1024.

SEEBURGER AG Vorstand/SEEBURGER Executive Board:
Sitz der Gesellschaft/Registered Office: Axel Haas, Michael Kleeberg, Friedemann Heinz, Dr. Martin Kuntz, Matthias Fe
Edisonstr. 1
D-75015 Bretten Vorsitzende des Aufsichtsrats/Chairperson of the SEEBURGER Supervisory Board:
Tel.: 07252 / 96 - 0 Prof. Dr. Simone Zeuchner
Fax: 07252 / 96 - 2222
Internet: https://na01.safelinks.protection.outlook.com/?
url=http%3A%2F%2Fwww.seeburger.de&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7C0480b4cbfcff443e0de708d5
Registergericht/Commercial Register:
e-mail: [hidden email]<mailto:[hidden email]> HRB 240708 Mannheim

Dieses E-Mail ist nur für den Empfänger bestimmt, an den es gerichtet ist und kann vertrauliches bzw. unter das Berufsgeheimni
Jegliche darin enthaltene Ansicht oder Meinungsäußerung ist die des Autors und stellt nicht notwendigerweise die Ansicht oder M
Sind Sie nicht der Empfänger, so haben Sie diese E-Mail irrtümlich erhalten und jegliche Verwendung, Veröffentlichung, Weiterle
Druck dieser E-Mail ist strengstens untersagt. Weder die SEEBURGER AG noch der Absender (Eckenfels. Bernd) übernehmen die
Verantwortung, die E-Mail und deren Anhänge auf Viren zu prüfen.

This email is intended only for the recipient(s) to whom it is addressed. This email may contain confidential material that may be
Any fact or opinion contained, or expression of the material herein, does not necessarily reflect that of SEEBURGER AG. If you ar
received this email in error, any use, publication or distribution including forwarding, copying or printing is strictly prohibited. Ne
sender (Eckenfels. Bernd) accept liability for viruses; it is your responsibility to check this email and its attachments for viruses.

SEEBURGER AG Vorstand/SEEBURGER Executive Board:
Sitz der Gesellschaft/Registered Office: Axel Haas, Michael Kleeberg, Friedemann Heinz, Dr. Martin Kuntz, Matthias Fe
Edisonstr. 1
D-75015 Bretten Vorsitzende des Aufsichtsrats/Chairperson of the SEEBURGER Supervisory Board:
Tel.: 07252 / 96 - 0 Prof. Dr. Simone Zeuchner
Fax: 07252 / 96 - 2222
Internet: http://www.seeburger.de Registergericht/Commercial Register:
e-mail: [hidden email] HRB 240708 Mannheim

Dieses E-Mail ist nur für den Empfänger bestimmt, an den es gerichtet ist und kann vertrauliches bzw. unter das Berufsgeheimni
Jegliche darin enthaltene Ansicht oder Meinungsäußerung ist die des Autors und stellt nicht notwendigerweise die Ansicht oder M
Sind Sie nicht der Empfänger, so haben Sie diese E-Mail irrtümlich erhalten und jegliche Verwendung, Veröffentlichung, Weiterle
Druck dieser E-Mail ist strengstens untersagt. Weder die SEEBURGER AG noch der Absender (Eckenfels. Bernd) übernehmen die
Verantwortung, die E-Mail und deren Anhänge auf Viren zu prüfen.

This email is intended only for the recipient(s) to whom it is addressed. This email may contain confidential material that may be
Any fact or opinion contained, or expression of the material herein, does not necessarily reflect that of SEEBURGER AG. If you ar
received this email in error, any use, publication or distribution including forwarding, copying or printing is strictly prohibited. Ne
sender (Eckenfels. Bernd) accept liability for viruses; it is your responsibility to check this email and its attachments for viruses.

David Hook-3 Jun 26, 2018; 8:35pm **Re: FIPS Java API provider and non-FIPS provider**

253 posts

Yes, I'd say this more of a FIPS friendly solution. We haven't had any end users to date that have been happy with the idea of mixing a FIPS and non-FIPS API. As an example, if a key object might be used by a non-FIPS section of your application you've automatically blown compliance - this condition applies to anything recognised in the security policy as a critical security parameter (CSP). The BCFIPS API does make it possible for FIPS and non-FIPS to exist in different threads, but it does this by making sure CSPs can't be used across the boundary (it's one of the main reasons why we ended up doing it like we did).

The other issue with using the class loader is the JCE is inevitably loaded by the system class loader, the chance of a clash still exists as a result. You could probably quarantine the classes if you only used the FIPS low level API (which would reduce the chance of the system class loader trying to interact with the "wrong" one), but it would really be better to have a solution that draws a hard line between the FIPS world and the non-FIPS world.

As I mentioned earlier as well, if the bcprov dependency is one of the latest, there's a good chance migrating everything else to FIPS would not be that hard.

Regards,

David

On 27/06/18 08:07, Eckenfels. Bernd wrote:
... [show rest of quote]

Rhuberg,Anthony

Jun 26, 2018; 8:57pm **Re: FIPS Java API provider and non-FIPS provider**

15 posts

So taking a step back from the Fips and non Fios bouncy castle versions, it appears you would recommend regardless of the cry
Fips and non Fips compliant security providers. Is that true? Or is this only an issue because of the bouncy castle implementatio

We had considered a Fips only JVM, but started to go down the class loader path because it was just easier to implement (easier

From: David Hook <[hidden email]>
Sent: Tuesday, June 26, 2018 8:35:22 PM
To: [hidden email]
Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider

Yes, I'd say this more of a FIPS friendly solution. We haven't had any end users to date that have been happy with the idea of mixing a FIPS and non-FIPS API. As an example, if a key object might be used by a non-FIPS section of your application you've automatically blown compliance - this condition applies to anything recognised in the security policy as a critical security parameter (CSP). The BCFIPS API does make it possible for FIPS and non-FIPS to exist in different threads, but it does this by making sure CSPs can't be used across the boundary (it's one of the main reasons why we ended up doing it like we did).

The other issue with using the class loader is the JCE is inevitably loaded by the system class loader, the chance of a clash still exists as a result. You could probably quarantine the classes if you only used the FIPS low level API (which would reduce the chance of the system class loader trying to interact with the "wrong" one), but it would really be better to have a solution that draws a hard line between the FIPS world and the non-FIPS world.

As I mentioned earlier as well, if the bcprov dependency is one of the latest, there's a good chance migrating everything else to FIPS would not be that hard.

Regards,

David

On 27/06/18 08:07, Eckenfels. Bernd wrote:
> In your case I would put all the sensitive logic to sign and handle keys in a dedicated VM and use it via remote call.
clash but protects your keys much better, with the added benefit of beeing fully compliant with all requirements the F
used compliant. You can even limit admin access to the key store that way.
>

> Class loader tricks do not really work well for registered providers since they use the classloader from where they a
not work.
>
> Bernd
> --
> https://na01.safelinks.protection.outlook.com/?
url=http%3A%2F%2Fwww.seeburger.com&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7C6a8aa72c9574
> ____
> From: Rhuberg,Anthony [[hidden email]]
> Sent: Tuesday, June 26, 2018 23:22
> To: David Hook; Eckenfels. Bernd; [hidden email]
> Subject: RE: [dev-crypto] FIPS Java API provider and non-FIPS provider
>
> Hi,
>
> In our web application deployment within Tomcat, the bcprov.jar is loaded by both the common class loader and th
(both by third party dependencies). Our web application has a requirement to digitally sign a prescription (which is th
BC Java API). The entire application does not need to be FIPS compliant, just one of many workflows.
>
> Is the following a reasonable alternative to avoid the package clash?
>
>
>   1. Stop packaging bc-fips-1.0.1.jar in our web application (WAR) – the bcprov will exist in the common class load
loader
>   2. bc-fips-1.0.1.jar on the filesystem C:\fipsmodule
>   3. Create a URLClassLoader and load bc-fips-1.0.1.jar
>   4. Load the BouncyCastleFipsProvider class at runtime
>

```
>     public static final Provider getProvider() throws … {
>         List<URL> urls = new ArrayList();
>         for (File f : new File("C:/fipsmodule").listFiles()) {
>             urls.add(f.toURL());
>         }
>         URLClassLoader classLoader = new URLClassLoader(urls.stream().toArray(URL[]::new), null);
>         Provider provider = (Provider) classLoader
>                 .loadClass("org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider").newInstance();
>         return provider;
>     }
>
>     public byte[] sign(KeyStore keystore, String data) throws …{
>        Signature signature = Signature.getInstance(“SHA256withRSA”, getProvider());
>         signature.initSign((PrivateKey) keystore.getKey(getKeyAlias(), getKeystorePassword()));
>         signature.update(data.getBytes());
>         return signature.sign();
>     }
```

>
> Thanks
>
> From: David Hook [[hidden email]]
> Sent: Friday, June 22, 2018 6:13 PM
> To: Rhuberg,Anthony <[hidden email]>; [hidden email]; [hidden email]
> Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider
>
>
> Hi,
>
> Yes, the FIPS package cannot be changed as it would require revalidation, although that's really a financial, not a te
>
> There is a bit more to it though - the jars can't be used in the same application as it would make it almost impossib
was actually FIPS compliant. You would only need a 3rd party library to be calling the BC lightweight API to use a non
be all over. So they cannot co-exist, it just won't work like that.
>
> I'm happy to discuss this further off list, I'd just need a bit more background on what you're trying to do.
>
> Regards,
>
> David
>
> On 22/06/18 23:48, Rhuberg,Anthony wrote:
> Hi,
>
> I appreciate your help trying to resolve this conflict.
>
> Also, forgive my persistence.
>
> We require a FIPS compliant/validated crypto module. I do not think “spongycastle-like” is an alternative. We are ir
of our third parties already require use of the non-FIPS compliant jar (not something we can readily change). If I und
conflict seems to be an issue with common classes in either the bcfips and bcprov jars that contain the same classes v
(that are causing the name clashes). If these jars are never intended to be integrated with the same application, I su
limitation, but that probably makes it impossible to use the bcfips jar when other third parties (out of our/your contro
>

> Can the FIPS package not be changed because that would require it to be revalidated (by CMVP) ? What would be t
bcfips and bcprov to coexist? Maybe we could discuss this offline.
>
> Respectfully,
> Tony
>
>
> From: David Hook [[hidden email]]
> Sent: Thursday, June 21, 2018 4:22 AM
> To: Rhuberg,Anthony <[hidden email]><mailto:[hidden email]>; [hidden email]<mailto:[hidden email]>; [hidden
> Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider
>
>
> The FIPS package can't be changed. You could do a "spongycastle" on the original Bouncy Castle ones.
>
> The FIPS library doesn't have an implementation of the low-level BC library. From a FIPS point of view the low-leve
rules, and probably a couple they did not consider.
>
> Providers can certainly co-exist, but package name clashes (at least in the system class loader) are right out.
>
> Regards,
>
> David
>
> On 21/06/18 06:33, Rhuberg,Anthony wrote:
> Is it possible or an option to change the package names of bouncy castle fips implementation? Changing the name
provider that would not conflict with any other providers.
>
> ________________________________
> From: Rhuberg,Anthony <[hidden email]><mailto:[hidden email]>
> Sent: Wednesday, June 20, 2018 3:49:52 PM
> To: [hidden email]<mailto:[hidden email]>; [hidden email]<mailto:[hidden email]>
> Subject: RE: [dev-crypto] FIPS Java API provider and non-FIPS provider
>
> Thanks for the clarification. I found at least one class in the same package with a different implementation in bc-fip
that affects our workflow, but it explains the conflict.
>
>
> -----Original Message-----
> From: Eckenfels. Bernd [[hidden email]]
> Sent: Wednesday, June 20, 2018 3:19 PM
> To: [hidden email]<mailto:[hidden email]>
> Subject: RE: [dev-crypto] FIPS Java API provider and non-FIPS provider
>
> The problem is that BC and BcFiPS have conflicting implementation classes. There is some logic to that (be a plugin
seems to hurt more than it helps. Maybe it would be a option to offer a FIPS jar with distinct namespace for those cas
>
> --
> https://na01.safelinks.protection.outlook.com/?
url=http%3A%2F%2Fwww.seeburger.com&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7C0480b4cbfcff4
> ____________________________________
> From: Rhuberg,Anthony [[hidden email]<mailto:[hidden email]>]
> Sent: Wednesday, June 20, 2018 20:58
> To: David Hook; Matti Aarnio; [hidden email]<mailto:[hidden email]>
> Subject: RE: [dev-crypto] FIPS Java API provider and non-FIPS provider
>
> Hi again,
>
> I am trying to understand the conflict further and am not really familiar with JCA/JCE.
>
> If both JCE providers 'bcprov´and 'bcfips' are loaded into the same class loader, I do not understand the conflict if t
names and implementation classes. If I request a Signature.getinstance("SHA256withRSA", "BCFIPS"), would I not ge
NOT the bcprov instance?
>
> Can multiple JCE providers be deployed within an application and the application decide which implementation to us
expecting providers to coexist.
>
> Is this conflict a BC conflict only? I am asking because if we selected another JCE provider (to get around this issue
same class loader, would we still have a similar conflict between another provider and bcprov?
>
> Thanks again,
> Tony
>
> From: David Hook [[hidden email]]
> Sent: Tuesday, June 19, 2018 6:18 PM
> To: Rhuberg,Anthony <[hidden email]><mailto:[hidden email]>; Matti Aarnio <[hidden email]><mailto:[hidden en
[hidden email]>
> Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider
>
>
> The high risk element is the JCE - it depends how it gets loaded and if both things make use of the respective provi

end up in the system class loader and in that case there can be only one.
>
> If bcprov isn't loaded in the system class loader and/or bc-fips is able to satisfy the dependency anyway, you will pı
>
> General the problems you see if it is an issue don't make sense. You'll get issues with undefined methods, class not
cases you will get class cast exceptions where it seems impossible as well.
>
> If you want to ask the OpenSAML guys to talk to us we would be happy to help them update.
>
> Regards,
>
> David
>
> On 20/06/18 05:04, Rhuberg,Anthony wrote:
> Just a follow up from my previous question.
>
> We have a configuration with a Tomcat Valve which uses opensaml (with a dependency on xmlsec -> bcprov-jdk15
the root class loader (call it CLroot).
> We just started using bc-fips-1.0.1.jar for digital signatures in a web application. That jar is part of the war (call it C
>
> Based on this configuration, we expected to observe some conflict when executing the pathways for the Tomcat Val
>
> The applications are "working", but worry that there is some unseen or potential problem that we have just not enc
>
> Any thoughts? Do you have an examples of how a collision (between the 2 jars bcprov-jdk15on - bc-fips-1.0.1.jar)
have examples of typical errors when there is a conflict?
>
> Thanks,
> Tony
>
>
> From: Matti Aarnio [[hidden email]]
> Sent: Tuesday, June 05, 2018 2:33 PM
> To: Rhuberg,Anthony <[hidden email]><mailto:[hidden email]><mailto:[hidden email]><mailto:[hidden email]>;
email]><mailto:[hidden email]><mailto:[hidden email]>
> Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider
>
> Hi Tony,
>
> The detail that affects more than "in same JVM" is "are they in same class loader?"
>
> WARs are loaded into separate class loader chains.
> WAR1 gets loader chain: CL1, CLroot.
> WAR2 gets loader chain: CL2, CLroot.
>
> If neither BCFIPS nor BCPROV are in CLroot, and instead in separate WARs, then the libraries will not see each othe
>
> The "CLroot" is server/lib/ in current Tomcats.
> The "CLn" is webapps/warname/WEB-INF/lib/
>
> Best Regards, Matti
>
> On 05.06.2018 21:01, Rhuberg,Anthony wrote:
>
> We have an application deployed within Tomcat and that application is uses Apache CXF which has a dependency oı
>
> Referring to: https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.bouncycastle.org%2Ffips-java%2FBCFipsIn100.pdf&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7C0480b4cbfcff443e0de708d5d6e2
url=https%3A%2F%2Fwww.bouncycastle.org%2Ffips-java%2FBCFipsIn100.pdf&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7Ce60fa34500a84aeb1a7a08d5cb1
<https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.bouncycastle.org%2Ffips-java%2FBCFipsIn100.pdf&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7C0480b4cbfcff443e0de708d5d6e2
url=https%3A%2F%2Fwww.bouncycastle.org%2Ffips-java%2FBCFipsIn100.pdf&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7Ce60fa34500a84aeb1a7a08d5cb1
"The provider jar itself has no external dependencies, but it cannot be used in the same JVM as the regular Bouncy Ca
two jar files do not get along".
>
> We are integrating FIPS Java API provider into another application WAR. We have not encountered an issues yet, bı
errors are expected if two applications use different Bouncy Castle Java implementations within the same JVM.
>
> Thanks,Tony
>
>
>
> CONFIDENTIALITY NOTICE This message and any included attachments are from Cerner Corporation and are intenc
information contained in this message is confidential and may constitute inside or non-public information under intern
securities laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibite
are not the addressee, please promptly delete this message and notify the sender of the delivery error by e-mail or yc
offices in Kansas City, Missouri, U.S.A at (+1) (816)221-1024.
>
>

>
>
>
>
>
>
>
>
>
> SEEBURGER AG Vorstand/SEEBURGER Executive Board:
> Sitz der Gesellschaft/Registered Office: Axel Haas, Michael Kleeberg, Friedemann Heinz, Dr. Martin Kuntz
> Edisonstr. 1
> D-75015 Bretten Vorsitzende des Aufsichtsrats/Chairperson of the SEEBURGER Supervisory Board:
> Tel.: 07252 / 96 - 0 Prof. Dr. Simone Zeuchner
> Fax: 07252 / 96 - 2222
> Internet: https://na01.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.seeburger.de&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7C0480b4cbfcff443
Registergericht/Commercial Register:
> e-mail: [hidden email]<[hidden email]> HRB 240708 Mannheim
>
>
> Dieses E-Mail ist nur für den Empfänger bestimmt, an den es gerichtet ist und kann vertrauliches bzw. unter das Be
enthalten. Jegliche darin enthaltene Ansicht oder Meinungsäußerung ist die des Autors und stellt nicht notwendigerwe
SEEBURGER AG dar. Sind Sie nicht der Empfänger, so haben Sie diese E-Mail irrtümlich erhalten und jegliche Verwend
Weiterleitung, Abschrift oder jeglicher Druck dieser E-Mail ist strengstens untersagt. Weder die SEEBURGER AG noch
übernehmen die Haftung für Viren; es obliegt Ihrer Verantwortung, die E-Mail und deren Anhänge auf Viren zu prüfen
>
>
> This email is intended only for the recipient(s) to whom it is addressed. This email may contain confidential materia
professional secrecy. Any fact or opinion contained, or expression of the material herein, does not necessarily reflect t
are not the addressee or if you have received this email in error, any use, publication or distribution including forward
strictly prohibited. Neither SEEBURGER AG, nor the sender (Eckenfels. Bernd) accept liability for viruses; it is your res
and its attachments for viruses.
>
>
>
>
>
>
>
>
>
>
>
>
>
>
>
>
> SEEBURGER AG Vorstand/SEEBURGER Executive Board:
> Sitz der Gesellschaft/Registered Office: Axel Haas, Michael Kleeberg, Friedemann Heinz, Dr. Martin Kuntz
> Edisonstr. 1
> D-75015 Bretten Vorsitzende des Aufsichtsrats/Chairperson of the SEEBURGER Supervisory Board:
> Tel.: 07252 / 96 - 0 Prof. Dr. Simone Zeuchner
> Fax: 07252 / 96 - 2222
> Internet: https://na01.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.seeburger.de&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7C6a8aa72c95744c
Registergericht/Commercial Register:
> e-mail: [hidden email] HRB 240708 Mannheim
>
>
> Dieses E-Mail ist nur für den Empfänger bestimmt, an den es gerichtet ist und kann vertrauliches bzw. unter das Be
enthalten. Jegliche darin enthaltene Ansicht oder Meinungsäußerung ist die des Autors und stellt nicht notwendigerwe
SEEBURGER AG dar. Sind Sie nicht der Empfänger, so haben Sie diese E-Mail irrtümlich erhalten und jegliche Verwend
Weiterleitung, Abschrift oder jeglicher Druck dieser E-Mail ist strengstens untersagt. Weder die SEEBURGER AG noch
übernehmen die Haftung für Viren; es obliegt Ihrer Verantwortung, die E-Mail und deren Anhänge auf Viren zu prüfen
>
>
> This email is intended only for the recipient(s) to whom it is addressed. This email may contain confidential materia
professional secrecy. Any fact or opinion contained, or expression of the material herein, does not necessarily reflect t
are not the addressee or if you have received this email in error, any use, publication or distribution including forward
strictly prohibited. Neither SEEBURGER AG, nor the sender (Eckenfels. Bernd) accept liability for viruses; it is your res
and its attachments for viruses.
>
>
>

Rhuberg,Anthony Jun 26, 2018; 9:01pm **Re: FIPS Java API provider and non-FIPS provider**

15 posts

In reply to this post by David Hook-3

We would prefer not mixing. It just not seem that we could affect change of the third parties within the timeframe we have.

From: David Hook <[hidden email]>
Sent: Tuesday, June 26, 2018 8:35:22 PM
To: [hidden email]
Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider

Yes, I'd say this more of a FIPS friendly solution. We haven't had any end users to date that have been happy with the idea of mixing a FIPS and non-FIPS API. As an example, if a key object might be used by a non-FIPS section of your application you've automatically blown compliance - this condition applies to anything recognised in the security policy as a critical security parameter (CSP). The BCFIPS API does make it possible for FIPS and non-FIPS to exist in different threads, but it does this by making sure CSPs can't be used across the boundary (it's one of the main reasons why we ended up doing it like we did).

The other issue with using the class loader is the JCE is inevitably loaded by the system class loader, the chance of a clash still exists as a result. You could probably quarantine the classes if you only used the FIPS low level API (which would reduce the chance of the system class loader trying to interact with the "wrong" one), but it would really be better to have a solution that draws a hard line between the FIPS world and the non-FIPS world.

As I mentioned earlier as well, if the bcprov dependency is one of the latest, there's a good chance migrating everything else to FIPS would not be that hard.

Regards,

David

On 27/06/18 08:07, Eckenfels. Bernd wrote:
> In your case I would put all the sensitive logic to sign and handle keys in a dedicated VM and use it via remote call.
clash but protects your keys much better, with the added benefit of beeing fully compliant with all requirements the F
used compliant. You can even limit admin access to the key store that way.
>
> Class loader tricks do not really work well for registered providers since they use the classloader from where they a
not work.
>
> Bernd
> --
> https://na01.safelinks.protection.outlook.com/?
url=http%3A%2F%2Fwww.seeburger.com&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7C6a8aa72c9574
> ____________________________________
> From: Rhuberg,Anthony [[hidden email]]
> Sent: Tuesday, June 26, 2018 23:22
> To: David Hook; Eckenfels. Bernd; [hidden email]
> Subject: RE: [dev-crypto] FIPS Java API provider and non-FIPS provider
>
> Hi,
>
> In our web application deployment within Tomcat, the bcprov.jar is loaded by both the common class loader and th
(both by third party dependencies). Our web application has a requirement to digitally sign a prescription (which is th
BC Java API). The entire application does not need to be FIPS compliant, just one of many workflows.
>
> Is the following a reasonable alternative to avoid the package clash?
>
>
>   1. Stop packaging bc-fips-1.0.1.jar in our web application (WAR) – the bcprov will exist in the common class load
loader
>   2. bc-fips-1.0.1.jar on the filesystem C:\fipsmodule
>   3. Create a URLClassLoader and load bc-fips-1.0.1.jar
>   4. Load the BouncyCastleFipsProvider class at runtime
>

```
>     public static final Provider getProvider() throws … {
>         List<URL> urls = new ArrayList();
>         for (File f : new File("C:/fipsmodule").listFiles()) {
>             urls.add(f.toURL());
>         }
>         URLClassLoader classLoader = new URLClassLoader(urls.stream().toArray(URL[]::new), null);
>         Provider provider = (Provider) classLoader
>                 .loadClass("org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider").newInstance();
>         return provider;
>     }
>
>     public byte[] sign(KeyStore keystore, String data) throws …{
>        Signature signature = Signature.getInstance(“SHA256withRSA”, getProvider());
>         signature.initSign((PrivateKey) keystore.getKey(getKeyAlias(), getKeystorePassword()));
>         signature.update(data.getBytes());
>         return signature.sign();
>     }
>
```

> Thanks
>
> From: David Hook [[hidden email]]
> Sent: Friday, June 22, 2018 6:13 PM
> To: Rhuberg,Anthony <[hidden email]>; [hidden email]; [hidden email]
> Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider
>
>
> Hi,
>
> Yes, the FIPS package cannot be changed as it would require revalidation, although that's really a financial, not a te
>
> There is a bit more to it though - the jars can't be used in the same application as it would make it almost impossib
was actually FIPS compliant. You would only need a 3rd party library to be calling the BC lightweight API to use a non
be all over. So they cannot co-exist, it just won't work like that.
>
> I'm happy to discuss this further off list, I'd just need a bit more background on what you're trying to do.
>
> Regards,
>
> David
>
> On 22/06/18 23:48, Rhuberg,Anthony wrote:
> Hi,
>
> I appreciate your help trying to resolve this conflict.
>
> Also, forgive my persistence.
>
> We require a FIPS compliant/validated crypto module. I do not think “spongycastle-like” is an alternative. We are ir
of our third parties already require use of the non-FIPS compliant jar (not something we can readily change). If I und
conflict seems to be an issue with common classes in either the bcfips and bcprov jars that contain the same classes v
(that are causing the name clashes). If these jars are never intended to be integrated with the same application, I sup
limitation, but that probably makes it impossible to use the bcfips jar when other third parties (out of our/your contro
>
> Can the FIPS package not be changed because that would require it to be revalidated (by CMVP) ? What would be t
bcfips and bcprov to coexist? Maybe we could discuss this offline.
>
> Respectfully,
> Tony
>
>
> From: David Hook [[hidden email]]
> Sent: Thursday, June 21, 2018 4:22 AM
> To: Rhuberg,Anthony <[hidden email]><mailto:[hidden email]>; [hidden email]<mailto:[hidden email]>; [hidden
> Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider
>
>
> The FIPS package can't be changed. You could do a "spongycastle" on the original Bouncy Castle ones.
>
> The FIPS library doesn't have an implementation of the low-level BC library. From a FIPS point of view the low-leve
rules, and probably a couple they did not consider.
>
> Providers can certainly co-exist, but package name clashes (at least in the system class loader) are right out.
>
> Regards,
>
> David
>
> On 21/06/18 06:33, Rhuberg,Anthony wrote:
> Is it possible or an option to change the package names of bouncy castle fips implementation? Changing the name
provider that would not conflict with any other providers.
>
> ________________________________
> From: Rhuberg,Anthony <[hidden email]><mailto:[hidden email]>
> Sent: Wednesday, June 20, 2018 3:49:52 PM
> To: [hidden email]<mailto:[hidden email]>; [hidden email]<mailto:[hidden email]>
> Subject: RE: [dev-crypto] FIPS Java API provider and non-FIPS provider
>
> Thanks for the clarification. I found at least one class in the same package with a different implementation in bc-fip
that affects our workflow, but it explains the conflict.

>
>
> -----Original Message-----
> From: Eckenfels. Bernd [[hidden email]]
> Sent: Wednesday, June 20, 2018 3:19 PM
> To: [hidden email]<mailto:[hidden email]>
> Subject: RE: [dev-crypto] FIPS Java API provider and non-FIPS provider
>
> The problem is that BC and BcFiPS have conflicting implementation classes. There is some logic to that (be a plugin
seems to hurt more than it helps. Maybe it would be a option to offer a FIPS jar with distinct namespace for those cas
>
> --
> https://na01.safelinks.protection.outlook.com/?
url=http%3A%2F%2Fwww.seeburger.com&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7C0480b4cbfcff4
> ____
> From: Rhuberg,Anthony [[hidden email]<mailto:[hidden email]>]
> Sent: Wednesday, June 20, 2018 20:58
> To: David Hook; Matti Aarnio; [hidden email]<mailto:[hidden email]>
> Subject: RE: [dev-crypto] FIPS Java API provider and non-FIPS provider
>
> Hi again,
>
> I am trying to understand the conflict further and am not really familiar with JCA/JCE.
>
> If both JCE providers 'bcprov´and 'bcfips' are loaded into the same class loader, I do not understand the conflict if t
names and implementation classes. If I request a Signature.getinstance("SHA256withRSA", "BCFIPS"), would I not ge
NOT the bcprov instance?
>
> Can multiple JCE providers be deployed within an application and the application decide which implementation to us
expecting providers to coexist.
>
> Is this conflict a BC conflict only? I am asking because if we selected another JCE provider (to get around this issue
same class loader, would we still have a similar conflict between another provider and bcprov?
>
> Thanks again,
> Tony
>
> From: David Hook [[hidden email]]
> Sent: Tuesday, June 19, 2018 6:18 PM
> To: Rhuberg,Anthony <[hidden email]><mailto:[hidden email]>; Matti Aarnio <[hidden email]><mailto:[hidden e
[hidden email]>
> Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider
>
>
> The high risk element is the JCE - it depends how it gets loaded and if both things make use of the respective provi
end up in the system class loader and in that case there can be only one.
>
> If bcprov isn't loaded in the system class loader and/or bc-fips is able to satisfy the dependency anyway, you will pr
>
> General the problems you see if it is an issue don't make sense. You'll get issues with undefined methods, class not
cases you will get class cast exceptions where it seems impossible as well.
>
> If you want to ask the OpenSAML guys to talk to us we would be happy to help them update.
>
> Regards,
>
> David
>
> On 20/06/18 05:04, Rhuberg,Anthony wrote:
> Just a follow up from my previous question.
>
> We have a configuration with a Tomcat Valve which uses opensaml (with a dependency on xmlsec -> bcprov-jdk15
the root class loader (call it CLroot).
> We just started using bc-fips-1.0.1.jar for digital signatures in a web application. That jar is part of the war (call it C
>
> Based on this configuration, we expected to observe some conflict when executing the pathways for the Tomcat Val
>
> The applications are "working", but worry that there is some unseen or potential problem that we have just not enc
>
> Any thoughts? Do you have an examples of how a collision (between the 2 jars bcprov-jdk15on - bc-fips-1.0.1.jar)
have examples of typical errors when there is a conflict?
>
> Thanks,
> Tony
>
>
> From: Matti Aarnio [[hidden email]]
> Sent: Tuesday, June 05, 2018 2:33 PM
> To: Rhuberg,Anthony <[hidden email]><mailto:[hidden email]><mailto:[hidden email]><mailto:[hidden email]>;
email]><mailto:[hidden email]><mailto:[hidden email]>
> Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider

>
> Hi Tony,
>
> The detail that affects more than "in same JVM" is "are they in same class loader?"
>
> WARs are loaded into separate class loader chains.
> WAR1 gets loader chain: CL1, CLroot.
> WAR2 gets loader chain: CL2, CLroot.
>
> If neither BCFIPS nor BCPROV are in CLroot, and instead in separate WARs, then the libraries will not see each othe
>
> The "CLroot" is server/lib/ in current Tomcats.
> The "CLn" is webapps/warname/WEB-INF/lib/
>
> Best Regards, Matti
>
> On 05.06.2018 21:01, Rhuberg,Anthony wrote:
>
> We have an application deployed within Tomcat and that application is uses Apache CXF which has a dependency o
>
> Referring to: https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.bouncycastle.org%2Ffips-java%2FBCFipsIn100.pdf&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7C0480b4cbfcff443e0de708d5d6e2
url=https%3A%2F%2Fwww.bouncycastle.org%2Ffips-java%2FBCFipsIn100.pdf&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7Ce60fa34500a84aeb1a7a08d5cb1
<https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.bouncycastle.org%2Ffips-java%2FBCFipsIn100.pdf&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7C0480b4cbfcff443e0de708d5d6e2
url=https%3A%2F%2Fwww.bouncycastle.org%2Ffips-java%2FBCFipsIn100.pdf&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7Ce60fa34500a84aeb1a7a08d5cb1
"The provider jar itself has no external dependencies, but it cannot be used in the same JVM as the regular Bouncy Ca
two jar files do not get along".
>
> We are integrating FIPS Java API provider into another application WAR. We have not encountered an issues yet, bu
errors are expected if two applications use different Bouncy Castle Java implementations within the same JVM.
>
> Thanks,Tony
>
>
>
> CONFIDENTIALITY NOTICE This message and any included attachments are from Cerner Corporation and are intenc
information contained in this message is confidential and may constitute inside or non-public information under intern
securities laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibite
are not the addressee, please promptly delete this message and notify the sender of the delivery error by e-mail or yo
offices in Kansas City, Missouri, U.S.A at (+1) (816)221-1024.
>
>
>
>
>
>
>
>
>
>
>
> SEEBURGER AG   Vorstand/SEEBURGER Executive Board:
> Sitz der Gesellschaft/Registered Office: Axel Haas, Michael Kleeberg, Friedemann Heinz, Dr. Martin Kuntz
> Edisonstr. 1
> D-75015 Bretten   Vorsitzende des Aufsichtsrats/Chairperson of the SEEBURGER Supervisory Board:
> Tel.: 07252 / 96 - 0   Prof. Dr. Simone Zeuchner
> Fax: 07252 / 96 - 2222
> Internet: https://na01.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.seeburger.de&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7C0480b4cbfcff443
Registergericht/Commercial Register:
> e-mail: [hidden email]<[hidden email]>   HRB 240708 Mannheim
>
>
> Dieses E-Mail ist nur für den Empfänger bestimmt, an den es gerichtet ist und kann vertrauliches bzw. unter das Be
enthalten. Jegliche darin enthaltene Ansicht oder Meinungsäußerung ist die des Autors und stellt nicht notwendigerwe
SEEBURGER AG dar. Sind Sie nicht der Empfänger, so haben Sie diese E-Mail irrtümlich erhalten und jegliche Verwend
Weiterleitung, Abschrift oder jeglicher Druck dieser E-Mail ist strengstens untersagt. Weder die SEEBURGER AG noch
übernehmen die Haftung für Viren; es obliegt Ihrer Verantwortung, die E-Mail und deren Anhänge auf Viren zu prüfen
>
>
> This email is intended only for the recipient(s) to whom it is addressed. This email may contain confidential materia
professional secrecy. Any fact or opinion contained, or expression of the material herein, does not necessarily reflect t
are not the addressee or if you have received this email in error, any use, publication or distribution including forward
strictly prohibited. Neither SEEBURGER AG, nor the sender (Eckenfels. Bernd) accept liability for viruses; it is your res
and its attachments for viruses.
>
>
>

>
>
>
>
>
>
>
>
>
>
>
>
>
> SEEBURGER AG   Vorstand/SEEBURGER Executive Board:
> Sitz der Gesellschaft/Registered Office: Axel Haas, Michael Kleeberg, Friedemann Heinz, Dr. Martin Kuntz
> Edisonstr. 1
> D-75015 Bretten   Vorsitzende des Aufsichtsrats/Chairperson of the SEEBURGER Supervisory Board:
> Tel.: 07252 / 96 - 0   Prof. Dr. Simone Zeuchner
> Fax: 07252 / 96 - 2222
> Internet: https://na01.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.seeburger.de&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7C6a8aa72c95744c
Registergericht/Commercial Register:
> e-mail: [hidden email]   HRB 240708 Mannheim
>
>
> Dieses E-Mail ist nur für den Empfänger bestimmt, an den es gerichtet ist und kann vertrauliches bzw. unter das Be
enthalten. Jegliche darin enthaltene Ansicht oder Meinungsäußerung ist die des Autors und stellt nicht notwendigerwe
SEEBURGER AG dar. Sind Sie nicht der Empfänger, so haben Sie diese E-Mail irrtümlich erhalten und jegliche Verwend
Weiterleitung, Abschrift oder jeglicher Druck dieser E-Mail ist strengstens untersagt. Weder die SEEBURGER AG noch d
übernehmen die Haftung für Viren; es obliegt Ihrer Verantwortung, die E-Mail und deren Anhänge auf Viren zu prüfen
>
>
> This email is intended only for the recipient(s) to whom it is addressed. This email may contain confidential materia
professional secrecy. Any fact or opinion contained, or expression of the material herein, does not necessarily reflect t
are not the addressee or if you have received this email in error, any use, publication or distribution including forward
strictly prohibited. Neither SEEBURGER AG, nor the sender (Eckenfels. Bernd) accept liability for viruses; it is your res
and its attachments for viruses.
>
>
>

Rhuberg,Anthony

Jun 27, 2018; 12:32am **Re: FIPS Java API provider and non-FIPS provider**

15 posts

In reply to this post by Eckenfels. Bernd

What do you mean by 'registered providers'?

Thanks

From: Eckenfels. Bernd <[hidden email]>
Sent: Tuesday, June 26, 2018 6:07:09 PM
To: [hidden email]
Subject: RE: [dev-crypto] FIPS Java API provider and non-FIPS provider

In your case I would put all the sensitive logic to sign and handle keys in a dedicated VM and use it via remote call. Tl
clash but protects your keys much better, with the added benefit of beeing fully compliant with all requirements the F
used compliant. You can even limit admin access to the key store that way.

Class loader tricks do not really work well for registered providers since they use the classloader from where they are
work.

Bernd
--
https://na01.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.seeburger.com&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7Ccd7d63253211

From: Rhuberg,Anthony [[hidden email]]
Sent: Tuesday, June 26, 2018 23:22
To: David Hook; Eckenfels. Bernd; [hidden email]
Subject: RE: [dev-crypto] FIPS Java API provider and non-FIPS provider

Hi,

In our web application deployment within Tomcat, the bcprov.jar is loaded by both the common class loader and the w
(both by third party dependencies). Our web application has a requirement to digitally sign a prescription (which is th

BC Java API). The entire application does not need to be FIPS compliant, just one of many workflows.

Is the following a reasonable alternative to avoid the package clash?

1. Stop packaging bc-fips-1.0.1.jar in our web application (WAR) – the bcprov will exist in the common class loader
2. bc-fips-1.0.1.jar on the filesystem C:\fipsmodule
3. Create a URLClassLoader and load bc-fips-1.0.1.jar
4. Load the BouncyCastleFipsProvider class at runtime

```
public static final Provider getProvider() throws … {
    List<URL> urls = new ArrayList();
    for (File f : new File("C:/fipsmodule").listFiles()) {
        urls.add(f.toURL());
    }
    URLClassLoader classLoader = new URLClassLoader(urls.stream().toArray(URL[]::new), null);
    Provider provider = (Provider) classLoader
            .loadClass("org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider").newInstance();
    return provider;
}

public byte[] sign(KeyStore keystore, String data) throws …{
   Signature signature = Signature.getInstance(“SHA256withRSA”, getProvider());
    signature.initSign((PrivateKey) keystore.getKey(getKeyAlias(), getKeystorePassword()));
    signature.update(data.getBytes());
    return signature.sign();
}
```

Thanks

From: David Hook [[hidden email]]
Sent: Friday, June 22, 2018 6:13 PM
To: Rhuberg,Anthony <[hidden email]>; [hidden email]; [hidden email]
Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider

Hi,

Yes, the FIPS package cannot be changed as it would require revalidation, although that's really a financial, not a tech

There is a bit more to it though - the jars can't be used in the same application as it would make it almost impossible
was actually FIPS compliant. You would only need a 3rd party library to be calling the BC lightweight API to use a non
be all over. So they cannot co-exist, it just won't work like that.

I'm happy to discuss this further off list, I'd just need a bit more background on what you're trying to do.

Regards,

David

On 22/06/18 23:48, Rhuberg,Anthony wrote:
Hi,

I appreciate your help trying to resolve this conflict.

Also, forgive my persistence.

We require a FIPS compliant/validated crypto module. I do not think “spongycastle-like” is an alternative. We are incl
our third parties already require use of the non-FIPS compliant jar (not something we can readily change). If I unders
seems to be an issue with common classes in either the bcfips and bcprov jars that contain the same classes with diff
causing the name clashes). If these jars are never intended to be integrated with the same application, I suppose I ur
that probably makes it impossible to use the bcfips jar when other third parties (out of our/your control) use the non-

Can the FIPS package not be changed because that would require it to be revalidated (by CMVP) ? What would be the
bcfips and bcprov to coexist? Maybe we could discuss this offline.

Respectfully,
Tony

From: David Hook [[hidden email]]
Sent: Thursday, June 21, 2018 4:22 AM
To: Rhuberg,Anthony <[hidden email]><mailto:[hidden email]>; [hidden email]<mailto:[hidden email]>; [hidden er
Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider

The FIPS package can't be changed. You could do a "spongycastle" on the original Bouncy Castle ones.

The FIPS library doesn't have an implementation of the low-level BC library. From a FIPS point of view the low-level A
rules, and probably a couple they did not consider.

Providers can certainly co-exist, but package name clashes (at least in the system class loader) are right out.

Regards,

David

On 21/06/18 06:33, Rhuberg,Anthony wrote:
Is it possible or an option to change the package names of bouncy castle fips implementation? Changing the name wc
provider that would not conflict with any other providers.

____
From: Rhuberg,Anthony <[hidden email]><mailto:[hidden email]>
Sent: Wednesday, June 20, 2018 3:49:52 PM
To: [hidden email]<mailto:[hidden email]>; [hidden email]<mailto:[hidden email]>
Subject: RE: [dev-crypto] FIPS Java API provider and non-FIPS provider

Thanks for the clarification. I found at least one class in the same package with a different implementation in bc-fips t
affects our workflow, but it explains the conflict.

-----Original Message-----
From: Eckenfels. Bernd [[hidden email]]
Sent: Wednesday, June 20, 2018 3:19 PM
To: [hidden email]<mailto:[hidden email]>
Subject: RE: [dev-crypto] FIPS Java API provider and non-FIPS provider

The problem is that BC and BcFiPS have conflicting implementation classes. There is some logic to that (be a plugin re
to hurt more than it helps. Maybe it would be a option to offer a FIPS jar with distinct namespace for those cases.

--
https://na01.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.seeburger.com&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7C0480b4cbfcff4
____
From: Rhuberg,Anthony [[hidden email]<mailto:[hidden email]>]
Sent: Wednesday, June 20, 2018 20:58
To: David Hook; Matti Aarnio; [hidden email]<mailto:[hidden email]>
Subject: RE: [dev-crypto] FIPS Java API provider and non-FIPS provider

Hi again,

I am trying to understand the conflict further and am not really familiar with JCA/JCE.

If both JCE providers 'bcprov´and 'bcfips' are loaded into the same class loader, I do not understand the conflict if the
names and implementation classes. If I request a Signature.getinstance("SHA256withRSA", "BCFIPS"), would I not ge
NOT the bcprov instance?

Can multiple JCE providers be deployed within an application and the application decide which implementation to use
expecting providers to coexist.

Is this conflict a BC conflict only? I am asking because if we selected another JCE provider (to get around this issue) a
class loader, would we still have a similar conflict between another provider and bcprov?

Thanks again,
Tony

From: David Hook [[hidden email]]
Sent: Tuesday, June 19, 2018 6:18 PM
To: Rhuberg,Anthony <[hidden email]><mailto:[hidden email]>; Matti Aarnio <[hidden email]><mailto:[hidden ema
[hidden email]>
Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider

The high risk element is the JCE - it depends how it gets loaded and if both things make use of the respective provide
up in the system class loader and in that case there can be only one.

If bcprov isn't loaded in the system class loader and/or bc-fips is able to satisfy the dependency anyway, you will prob

General the problems you see if it is an issue don't make sense. You'll get issues with undefined methods, class not fc
cases you will get class cast exceptions where it seems impossible as well.

If you want to ask the OpenSAML guys to talk to us we would be happy to help them update.

Regards,

David

On 20/06/18 05:04, Rhuberg,Anthony wrote:
Just a follow up from my previous question.

We have a configuration with a Tomcat Valve which uses opensaml (with a dependency on xmlsec -> bcprov-jdk15on
root class loader (call it CLroot).

We just started using bc-fips-1.0.1.jar for digital signatures in a web application. That jar is part of the war (call it CL

Based on this configuration, we expected to observe some conflict when executing the pathways for the Tomcat Valve

The applications are "working", but worry that there is some unseen or potential problem that we have just not encou

Any thoughts? Do you have an examples of how a collision (between the 2 jars bcprov-jdk15on - bc-fips-1.0.1.jar) w
examples of typical errors when there is a conflict?

Thanks,
Tony

From: Matti Aarnio [[hidden email]]
Sent: Tuesday, June 05, 2018 2:33 PM
To: Rhuberg,Anthony <[hidden email]><mailto:[hidden email]><mailto:[hidden email]><mailto:[hidden email]>; [h
email]><mailto:[hidden email]><mailto:[hidden email]>
Subject: Re: [dev-crypto] FIPS Java API provider and non-FIPS provider

Hi Tony,

The detail that affects more than "in same JVM" is "are they in same class loader?"

WARs are loaded into separate class loader chains.
WAR1 gets loader chain: CL1, CLroot.
WAR2 gets loader chain: CL2, CLroot.

If neither BCFIPS nor BCPROV are in CLroot, and instead in separate WARs, then the libraries will not see each other,

The "CLroot" is server/lib/ in current Tomcats.
The "CLn" is webapps/warname/WEB-INF/lib/

Best Regards, Matti

On 05.06.2018 21:01, Rhuberg,Anthony wrote:

We have an application deployed within Tomcat and that application is uses Apache CXF which has a dependency on b

Referring to: https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.bouncycastle.org%2Ffips-java%2FBCFipsIn100.pdf&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7C0480b4cbfcff443e0de708d5d6e2
url=https%3A%2F%2Fwww.bouncycastle.org%2Ffips-java%2FBCFipsIn100.pdf&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7Ce60fa34500a84aeb1a7a08d5cb1
<https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.bouncycastle.org%2Ffips-java%2FBCFipsIn100.pdf&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7C0480b4cbfcff443e0de708d5d6e2
url=https%3A%2F%2Fwww.bouncycastle.org%2Ffips-java%2FBCFipsIn100.pdf&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7Ce60fa34500a84aeb1a7a08d5cb1
"The provider jar itself has no external dependencies, but it cannot be used in the same JVM as the regular Bouncy Ca
two jar files do not get along".

We are integrating FIPS Java API provider into another application WAR. We have not encountered an issues yet, but
errors are expected if two applications use different Bouncy Castle Java implementations within the same JVM.

Thanks,Tony

CONFIDENTIALITY NOTICE This message and any included attachments are from Cerner Corporation and are intende
information contained in this message is confidential and may constitute inside or non-public information under intern
securities laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibite
are not the addressee, please promptly delete this message and notify the sender of the delivery error by e-mail or yo
offices in Kansas City, Missouri, U.S.A at (+1) (816)221-1024.

SEEBURGER AG Vorstand/SEEBURGER Executive Board:
Sitz der Gesellschaft/Registered Office: Axel Haas, Michael Kleeberg, Friedemann Heinz, Dr. Martin Kuntz, M
Edisonstr. 1
D-75015 Bretten Vorsitzende des Aufsichtsrats/Chairperson of the SEEBURGER Supervisory Board:
Tel.: 07252 / 96 - 0 Prof. Dr. Simone Zeuchner
Fax: 07252 / 96 - 2222
Internet: https://na01.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.seeburger.de&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7C0480b4cbfcff443
Registergericht/Commercial Register:

e-mail: [hidden email]<[hidden email]>   HRB 240708 Mannheim

Dieses E-Mail ist nur für den Empfänger bestimmt, an den es gerichtet ist und kann vertrauliches bzw. unter das Beru
enthalten. Jegliche darin enthaltene Ansicht oder Meinungsäußerung ist die des Autors und stellt nicht notwendigerwe
SEEBURGER AG dar. Sind Sie nicht der Empfänger, so haben Sie diese E-Mail irrtümlich erhalten und jegliche Verwen
Weiterleitung, Abschrift oder jeglicher Druck dieser E-Mail ist strengstens untersagt. Weder die SEEBURGER AG noch
übernehmen die Haftung für Viren; es obliegt Ihrer Verantwortung, die E-Mail und deren Anhänge auf Viren zu prüfen

This email is intended only for the recipient(s) to whom it is addressed. This email may contain confidential material t
professional secrecy. Any fact or opinion contained, or expression of the material herein, does not necessarily reflect t
are not the addressee or if you have received this email in error, any use, publication or distribution including forward
strictly prohibited. Neither SEEBURGER AG, nor the sender (Eckenfels. Bernd) accept liability for viruses; it is your res
and its attachments for viruses.

SEEBURGER AG   Vorstand/SEEBURGER Executive Board:
Sitz der Gesellschaft/Registered Office: Axel Haas, Michael Kleeberg, Friedemann Heinz, Dr. Martin Kuntz, M
Edisonstr. 1
D-75015 Bretten   Vorsitzende des Aufsichtsrats/Chairperson of the SEEBURGER Supervisory Board:
Tel.: 07252 / 96 - 0   Prof. Dr. Simone Zeuchner
Fax: 07252 / 96 - 2222
Internet: https://na01.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.seeburger.de&data=02%7C01%7CAnthony.Rhuberg%40Cerner.com%7Ccd7d632532114
Registergericht/Commercial Register:
e-mail: [hidden email]   HRB 240708 Mannheim

Dieses E-Mail ist nur für den Empfänger bestimmt, an den es gerichtet ist und kann vertrauliches bzw. unter das Beru
enthalten. Jegliche darin enthaltene Ansicht oder Meinungsäußerung ist die des Autors und stellt nicht notwendigerwe
SEEBURGER AG dar. Sind Sie nicht der Empfänger, so haben Sie diese E-Mail irrtümlich erhalten und jegliche Verwen
Weiterleitung, Abschrift oder jeglicher Druck dieser E-Mail ist strengstens untersagt. Weder die SEEBURGER AG noch
übernehmen die Haftung für Viren; es obliegt Ihrer Verantwortung, die E-Mail und deren Anhänge auf Viren zu prüfen

This email is intended only for the recipient(s) to whom it is addressed. This email may contain confidential material t
professional secrecy. Any fact or opinion contained, or expression of the material herein, does not necessarily reflect t
are not the addressee or if you have received this email in error, any use, publication or distribution including forward
strictly prohibited. Neither SEEBURGER AG, nor the sender (Eckenfels. Bernd) accept liability for viruses; it is your res
and its attachments for viruses.

« Return to Bouncy Castle - Dev | 579 views

Disable Popup Ads | Edit this page