

FIPS 140-2

Expectation Management

Jean Campbell

Communications Security Establishment

CMVP Symposium 2004

14 September 2004

Presentation Outline

- What FIPS 140-2 is
- What FIPS 140-2 isn't
 - Purpose of cryptographic module testing
 - cryptographic boundary
 - Roles and authentication
 - Porting
 - What to look for
- Conclusion

What FIPS 140-2 is

- NOT the panacea of all IT security problems...
 - but an important part of the security solution
- Sets the MINIMUM requirements for cryptographic products

... hence: *Where security starts...*

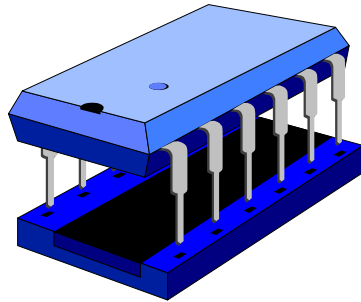
Purpose of Cryptographic Module Testing

- Confirmation of conformance to FIPS 140-2
 - Have the FIPS 140-2 requirements been met?
 - Same applies to algorithm validation testing
- It is not:
 - functionality testing (for non-cryptographic ones)
 - Interoperability testing
- Non-FIPS IT security functions are not tested

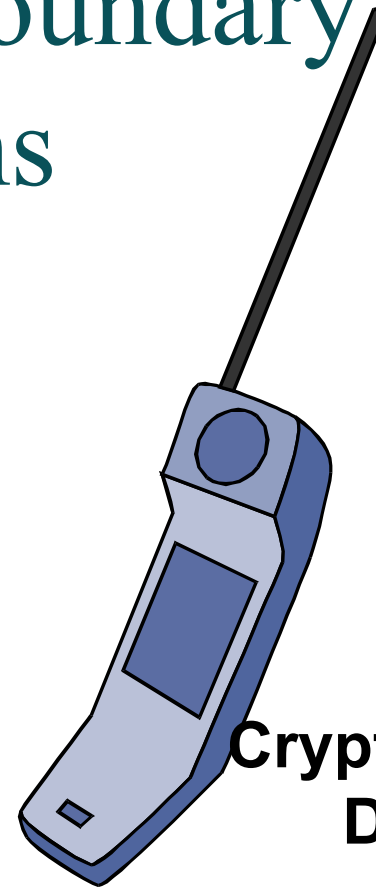
Cryptographic Boundary

- Defines the perimeter of the cryptographic module
 - May or may not be the entire “product”
- FIPS 140-2 requirements only apply to it
 - (e.g., input and output of CSP)
- Functionality that is outside the cryptographic boundary is “out of scope”
- Abstract for software modules
 - Logical and physical boundaries
- Described in the security policy

Cryptographic Boundary Illustrations



Cryptographic ASIC



Cryptographic Device

Cryptographic Boundary

- Defines the perimeter of the cryptographic module
 - May or may not be the entire “product”
- FIPS 140-2 requirements only apply to it
 - (e.g., input and output of CSP)
- Functionality that is outside the cryptographic boundary is “out of scope”
- Abstract for software modules
 - Logical and physical boundaries
- Described in the security policy

Porting

- Validation is maintained when module is operated unchanged on another OS or GPC (ref: IG G.5)
- Allowed based on the general premise that it will work on target OS or GPC
- Only allowed for validated version, no modification allowed
- Vendor claim-based, not tested
- For greater assurance, have it tested!

What to look for:

- Understand FIPS PUB 140-2
- CMVP Website and the *Validated ... FIPS 140-2 ... Module List*
 - <http://csrc.ncsl.nist.gov/cryptval/140-1/140val-all.htm>
 - Understand the information presented

447

[Oracle Corporation](#)

500 Oracle Parkway,
Redwood Shores,
California, CA
94065
USA

-[Shaun Lee](#)
TEL: +44 1189 243860

**Oracle Cryptographic Libraries for
SSL 10g (9.0.4)**

(Software Version 10g (9.0.4))

(When operated in FIPS mode)

Validated to FIPS 140-2

[Security Policy](#)

[Certificate](#)

Software

08/09/2004

Name of the module

Disclaimer
The use of the Oracle Corp.
validation certificate is for
example purposes only.

SanGuard 200 HTML provides secure
identity-based challenge-response
authentication using smart cards and
data encryption using FIPS approved
algorithms.

Tested as
meeting Level 2 with Sun Solaris
Version 8 running on a Sun Ultra 60
UltraSparc workstation

-*FIPS-approved algorithms:* DES
(Cert. #215); Triple-DES (Cert.
#170); SHA-1 (Cert. #154); RSA
(PKCS#1, vendor affirmed); HMAC-
SHA-1 (Cert. #154, vendor affirmed)
-*Other algorithms:* RSA-MD5
(PKCS#1); RC4; HMAC-MD5;
Diffie-Hellman (key agreement); RSA
(PKCS#5)

Multi-chip standalone

"The Oracle Cryptographic Libraries
for SSL 10g (9.0.4) is a generic
module used by Oracle Corporation in
a variety of its application suites. The
module is used to provide support to
cryptology, authentication, PKCS
and certificate management for
applications like the Oracle Database
Server, Oracle Applications Server,

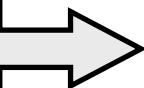
File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss

Address http://csrc.nist.gov/cryptval/140-1/140val-all.htm Go

447	<p>USA</p> <p>-Shaun Lee TEL: +44 1189 243860</p>	<p>Oracle Cryptographic Libraries for SSL 10g (9.0.4) (Software Version 10g (9.0.4)) <i>(When operated in FIPS mode)</i></p> <p>Validated to FIPS 140-2</p> <p>Security Policy</p> <p>Certificate</p>	Software	06/30/2004; 08/06/2004	<p>Overall Level: 2</p> <p>-Operational Environment: Tested as meeting Level 2 with Sun Solaris Version 8 running on a Sun Ultra 60 UltraSparc workstation</p> <p>-FIPS-approved algorithms: DES (Cert. #215); Triple-DES (Cert. #170); SHA-1 (Cert. #154); RSA (PKCS#1, vendor affirmed); HMAC-SHA-1 (Cert. #154, vendor affirmed)</p> <p>-Other algorithms: RSA-MD5 (PKCS#1); RC4; HMAC-MD5; Diffie-Hellman (key agreement); RSA (PKCS#5)</p> <p>Multi-chip standalone</p> <p>"The Oracle Cryptographic Libraries for SSL 10g (9.0.4) is a generic module used by Oracle Corporation in a variety of its application suites. The module is used to provide support to cryptography, authentication, PKCS and certificate management for applications like the Oracle Database Server, Oracle Applications Server,</p>
-----	---	---	----------	---------------------------	---

Version number of module



SSL 10g (9.0.4)
(Software Version 10g (9.0.4))
(When operated in FIPS mode)

Disclaimer

The use of the Oracle Corp. validation certificate is for example purposes only.

Validated 140-1 and 140-2 Cryptographic Modules (All) - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss

Address http://csrc.nist.gov/cryptval/140-1/140val-all.htm

447	Oracle Corporation 500 Oracle Parkway, Redwood City, CA 94065 -Shaun Lee TEL: +44 1189 243860	Oracle Cryptographic Libraries for SSL 10g (9.0.4) (Software Version 10g (9.0.4)) <i>(When operated in FIPS mode)</i> Validated to FIPS 140-2 Security Policy Certificate	Software	06/30/2004; 08/06/2004	<p>SunGuard 200 FIPS mode provides secure identity-based challenge-response authentication using smart cards and data encryption using FIPS approved 3DES and AES encryption."</p> <p>Overall Level: 2</p> <p>-Operational Environment: Tested as meeting Level 2 with Sun Solaris Version 8 running on a Sun Ultra 60 UltraSparc workstation</p> <p>-FIPS-approved algorithms: DES (Cert. #215); Triple-DES (Cert. #170); SHA-1 (Cert. #154); RSA (PKCS#1, vendor affirmed); HMAC-SHA-1 (Cert. #154, vendor affirmed)</p> <p>-Other algorithms: RSA-MD5 (PKCS#1); RC4; HMAC-MD5; Diffie-Hellman (key agreement); RSA (PKCS#5)</p> <p>Multi-chip standalone</p> <p>"The Oracle Cryptographic Libraries for SSL 10g (9.0.4) is a generic module used by Oracle Corporation in a variety of its application suites. The module is used to provide support to cryptography, authentication, PKCS and certificate management for applications like the Oracle Database Server, Oracle Applications Server,</p>
-----	---	--	----------	---------------------------	---

Non-FIPS Approved Mode Caveat

Disclaimer

The use of the Oracle Corp. validation certificate is for example purposes only.

447	<p>Oracle Corporation 500 Oracle Parkway, Redwood Shores, California , CA 94065 USA</p> <p>-Shaun Lee TEL: +44 1189 243860</p>	<p>Oracle Cryptographic Libraries for SSL 10g (9.0.4) (Software Version 10g (9.0.4)) <i>(When operated in FIPS mode)</i></p> <p>Validated to FIPS 140-2</p> <p>Security Policy</p> <p>Certificate</p>	<p>Software</p> <p>06/30/2004; 08/06/2004</p>	<p>Overall Level: 2</p> <p>-Operational Environment: Tested as meeting Level 2 with Sun Solaris Version 8 running on a Sun Ultra 60 UltraSparc workstation</p> <p><i>-FIPS-approved algorithms:</i> DES (Cert. #215); Triple-DES (Cert. #170); SHA-1 (Cert. #154); RSA (PKCS#1, vendor affirmed); HMAC-SHA-1 (Cert. #154, vendor affirmed)</p> <p><i>-Other algorithms:</i> RSA-MD5 (PKCS#1); RC4; HMAC-MD5; Diffie-Hellman (key agreement); RSA (PKCS#5)</p> <p>Multi-chip standalone</p> <p>"The Oracle Cryptographic Libraries for SSL 10g (9.0.4) is a generic module used by Oracle Corporation in a variety of its application suites. The module is used to provide support to cryptography, authentication, PKCS and certificate management for applications like the Oracle Database Server, Oracle Applications Server,</p>
-----	--	---	---	--

Approved cryptographic algorithms

-FIPS-approved algorithms: DES (Cert. #215); Triple-DES (Cert. #170); SHA-1 (Cert. #154); RSA (PKCS#1, vendor affirmed); HMAC-SHA-1 (Cert. #154, vendor affirmed)

Disclaimer

The use of the Oracle Corp. validation certificate is for example purposes only.

SanGuard 200 Home provides secure identity-based challenge-response authentication using smart cards and data encryption using FIPS approved 3DES and AES encryption."

447 [Oracle Corporation](#)
500 Oracle Parkway,
Redwood Shores,
California , CA
94065
USA

-[Shaun Lee](#)
TEL: +44 1189 243860

**Oracle Cryptographic Libraries for
SSL 10g (9.0.4)**
(Software Version 10g (9.0.4))

(When operated in FIPS mode)

Validated to FIPS 140-2

[Security Policy](#)

[Certificate](#)

Software 06/30/2004;
08/06/2004

Overall Level: 2

-Operational Environment: Tested as meeting Level 2 with Sun Solaris Version 8 running on a Sun Ultra 60 UltraSparc workstation

-FIPS-approved algorithms: DES (Cert. #215); Triple-DES (Cert. #170); SHA-1 (Cert. #154); RSA (PKCS#1 vendor affirmed); HMAC-SHA-1 (Cert. #154, vendor affirmed)
-Other algorithms: RSA-MD5 (PKCS#1); RC4; HMAC-MD5; Diffie-Hellman (key agreement); RSA (PKCS#5)

Multi-chip standalone

"The Oracle Cryptographic Libraries

**Non-Approved
cryptographic
algorithms**

Disclaimer
The use of the Oracle Corp. validation certificate is for example purposes only.

and certificate management for applications like the Oracle Database Server, Oracle Applications Server,

447	<p>Oracle Corporation 500 Oracle Parkway, Redwood Shores, California , CA 94065 USA</p> <p>-Shaun Lee TEL: +44 1189 243860</p>	<p>Oracle Cryptographic Libraries for SSL 10g (9.0.4) (Software (When operating)</p> <p>Validated to FIPS 140-2</p> <p>Security Policy</p> <p>Certificate</p>	<p>Software 06/30/2004; 08/06/2004</p>	<p>Overall Level: 2</p> <p>-Operational Environment: Tested as meeting Level 2 with Sun Solaris Version 8 running on a Sun Ultra 60 UltraSparc workstation</p> <p>-FIPS-approved algorithms: DES (Cert. #215); Triple-DES (Cert. #170); SHA-1 (Cert. #154); RSA (PKCS#1, vendor affirmed); HMAC-SHA-1 (Cert. #154, vendor affirmed)</p> <p>-Other algorithms: RSA-MD5 (PKCS#1); RC4; HMAC-MD5; Diffie-Hellman (key agreement); RSA (PKCS#5)</p> <p>Multi-chip standalone</p> <p>"The Oracle Cryptographic Libraries for SSL 10g (9.0.4) is a generic module used by Oracle Corporation in a variety of its application suites. The module is used to provide support to cryptography, authentication, PKCS and certificate management for applications like the Oracle Database Server, Oracle Applications Server,</p>
-----	--	---	--	---

Platform and OS used during testing

-Operational Environment: Tested as meeting Level 2 with Sun Solaris Version 8 running on a Sun Ultra 60 UltraSparc workstation

Disclaimer
The use of the Oracle Corp. validation certificate is for example purposes only.

SanGuard 200 from provides secure identity-based challenge-response authentication using smart cards and data encryption using FIPS approved 3DES and AES encryption."

447 [Oracle Corporation](#)
500 Oracle Parkway,
Redwood Shores,
California , CA
94065
USA

**Oracle Cryptographic Libraries for
SSL 10g (9.0.4)**
(Software Version 10g (9.0.4))
(When operated in FIPS mode)

Software 06/30/2004;
08/06/2004

Overall Level: 2

-Operational Environment: Tested as meeting Level 2 with Sun Solaris Version 8 running on a Sun Ultra 60 Ultra Sparc workstation

-[Shaun Lee](#)
TEL: +44 1189 243

Link to FIPS 140-2 Validation Certificate

Validated to FIPS 140-2

[Security Policy](#)
[Certificate](#)

Link to Security Policy document

-approved algorithms: DES (Cert. #215); Triple-DES (Cert. #154); SHA-1 (Cert. #154); RSA (Cert. #1, vendor affirmed); HMAC-SHA-1 (Cert. #154, vendor affirmed)

-Other algorithms: RSA-MD5 (PKCS#1); RC4; HMAC-MD5; Diffie-Hellman (key agreement); RSA (PKCS#5)

Multi-chip standalone

"The Oracle Cryptographic Libraries for SSL 10g (9.0.4) is a generic module used by Oracle Corporation in a variety of its application suites. The module is used to provide support to cryptography, authentication, PKCS and certificate management for applications like the Oracle Database Server, Oracle Applications Server,

Disclaimer
The use of the Oracle Corp. validation certificate is for example purposes only.

What to look for:

- Understand FIPS PUB 140-2
- CMVP Website and the *Validated ... FIPS 140-2 ... Module List*
 - www.nist.gov/cmvp
 - Understand the information presented
- Security Policy
 - What does it contain?

Security Policy Contents

- Non-proprietary document prepared by the vendor
- Version number of validated module and picture
- How to place the module in “FIPS Mode”
- Roles and authentication
- Approved and Non-Approved Cryptographic Functions
- Tested configuration (where applicable)
- Critical Security Parameters and access types
- Physical security policy
- Mitigation of Other Attacks (where applicable)

What to look for:

- Understand FIPS PUB 140-2
- CMVP Website and the *Validated ... FIPS 140-2 ... Module List*
 - www.nist.gov/cmvp
- Security Policy
 - What does it contain?
- Certificate
 - Benchmark of testing
 - Use website for current information

FIPS 140-2 Validation Certificate



The National Institute of Standards and Technology of the United States of America



Certificate No. 447



The Communications Security Establishment of the Government of Canada

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

Non-FIPS Approved
Mode Caveat

Oracle Cryptographic Libraries for SSL 10g (9.0.4) by Oracle Corporation

(When operated in FIPS mode)

Disclaimer

The use of the Oracle Corp. validation certificate is for example purposes only.

Derived Test Requirements for FIPS 140-2, *Security Requirements for Cryptographic Modules*. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Protected Information* (Canada) within computer and telecommunications systems

cryptographic module may be labeled as complying with the requirements of FIPS 140-2. This certificate continues to use the validated version of the cryptographic module as specified in the certificate. Additional details concerning test results. No reliability test has been performed. This is either expressed or implied.

Conformance and validation authority signatures on the reverse.

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module. The scope of conformance achieved by the cryptographic modules as tested in the product identified as:

**Oracle Cryptographic Libraries for SSL 10g (9.0.4) by Oracle Corporation
(Software Version 10g (9.0.4); Software)**

**LogicaCMG Security Consulting, NVLAP LAB CODE 200583-0,
CRYPTIK Version 5.8**

and tested by the Cryptographic Module Testing accredited laboratory:

is as follows:

Cryptographic Module Specification:

Level 2

Roles, Services, and Authentication:

Level 2

Physical Security:
(Multi-Chip Standalone)

Level N/A

EMI/EMC:

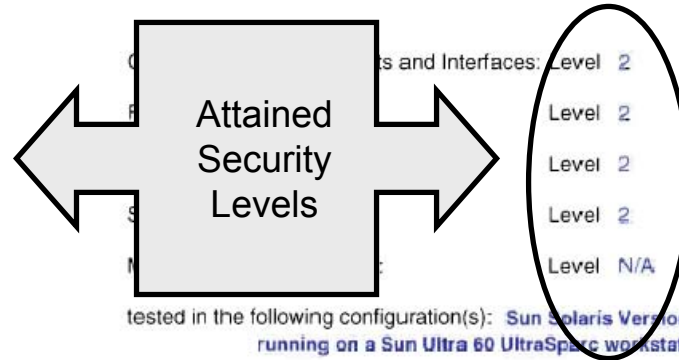
Level 2

Design Assurance:

Level 2

Operational Environment:

Level 2



The following FIPS approved Cryptographic Algorithms are used: **DES (Cert. #215); Triple-DES (Cert. #170); SHA-1 (Cert. #154); RSA (PKCS#1, vendor affirmed); HMAC-SHA-1 (Cert #154, vendor affirmed)**

The Cryptographic module also contains the following non-FIPS approved algorithms: **RSA-MD5 (PKCS#1); RC4; HMAC-MD5; Diffie-Hellman (key agreement); RSA (PKCS#5)**

Disclaimer

The use of the Oracle Corp. validation certificate is for example purposes only.

National Institute of Standards and Technology

Overall Level Achieved: 2

Signed on behalf of the Government of Canada

Signature: _____

Dated: _____

Director, Information Protection Group
The Communications Security Establishment

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module. The scope of conformance achieved by the cryptographic modules as tested in the product identified as:

**Oracle Cryptographic Libraries for SSL 10g (9.0.4) by Oracle Corporation
(Software Version 10g (9.0.4); Software)**

and tested by the Cryptographic Module Testing accredited laboratory: **LogicaCMG Security Consulting, NVLAP LAB CODE 200583-0,
CRYPTIK Version 5.8**

is as follows:

Cryptographic Module Specification:	Level 2	Cryptographic Module Ports and Interfaces:	Level 2
Roles, Services, and Authentication:	Level 2	Finite State Model:	Level 2
Physical Security: (Multi-Chip Standalone)	Level N/A	Cryptographic Key Management:	Level 2
EMI/EMC:	Level 2	Self Tests:	Level 2
Design Assurance:		Mitigation of Other Attacks:	Level N/A
Operational Environment:			

**Platform and OS
Used during
Testing**

in the following configuration(s): **Sun Solaris Version 8
running on a Sun Ultra 60 UltraSparc workstation**

The following FIPS approved Cryptographic Algorithms are used in the following configuration(s): **DES (Cert. #215); Triple-DES (Cert. #170); SHA-1 (Cert. #154); RSA (PKCS#1,
vendor affirmed); HMAC-SHA-1 (Cert #154, vendor affirmed)**

The Cryptographic module also contains the following non-FIPS approved algorithms: **RSA-MD5 (PKCS#1); RC4; HMAC-MD5; Diffie-Hellman
(key agreement); RSA (PKCS#5)**

Overall Level Achieved: 2

Disclaimer

The use of the Oracle Corp. validation certificate is for example purposes only.

National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: _____

Director, Information Protection Group
The Communications Security Establishment

Conclusion

- FIPS 140-2 is not the silver bullet: it is part of the overall solution
- Know what is validated: the cryptographic boundary
- Know where to get the information about the module:
 - www.nist.gov/cmvp
 - security policy
 - CMVP Frequently Asked Questions (FAQ)
- Call us if you have questions

Jean Campbell
Communications Security Establishment
☎: (613) 991-8121
🖱: Jean.Campbell@cse-cst.gc.ca

Randall J. Easter
National Institute of Standards and Technology
☎: (301) 975-4641
🖱: Randall.Easter@nist.gov