

ICCC11

CC's place  
in the security market



# Security market as seen from evaluation methodologies

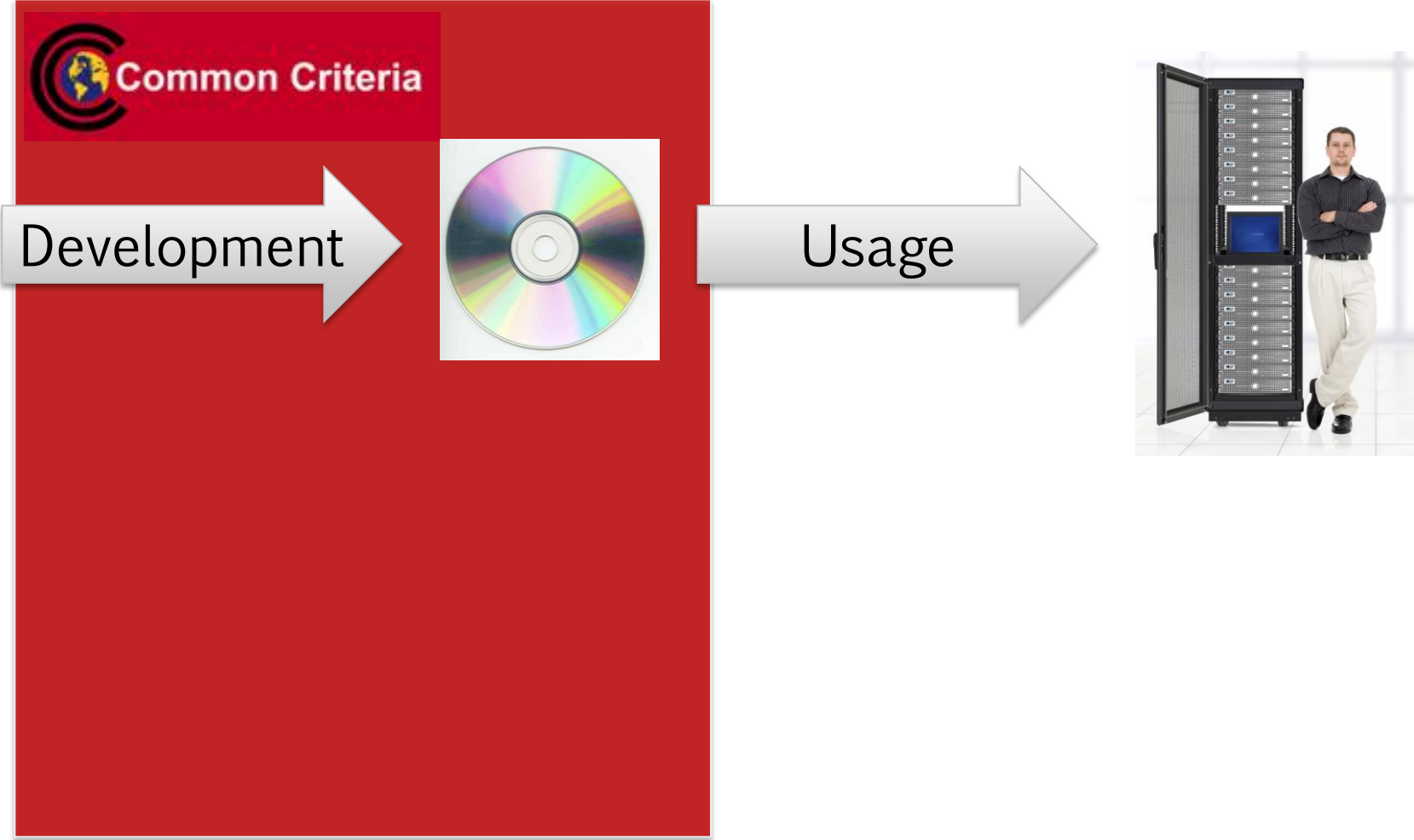
Development



Usage

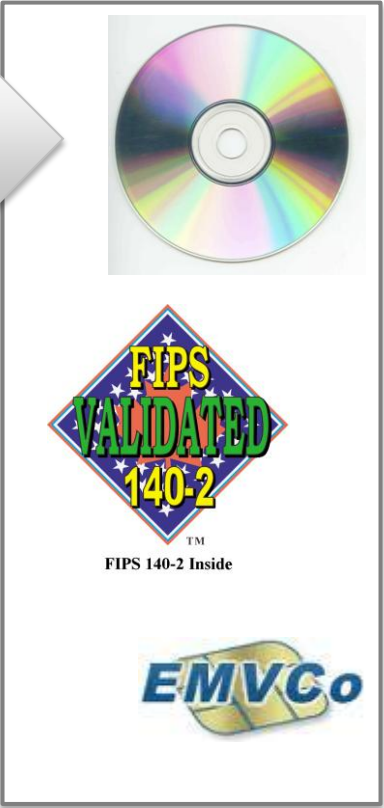


# Common Criteria



# Developed product focus

Development



Usage



# Deployed product focus

Development



Usage

A man in a dark shirt and light-colored trousers stands with his arms crossed next to a black server rack. The rack has its door open, revealing internal components. The background is a bright, slightly blurred office setting.

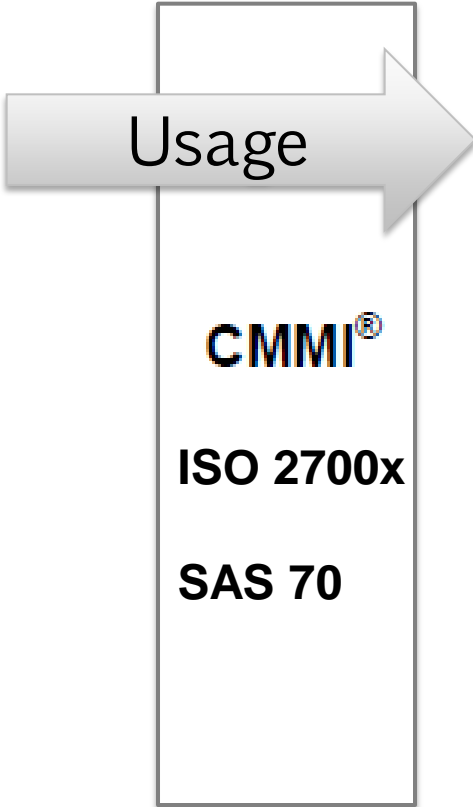
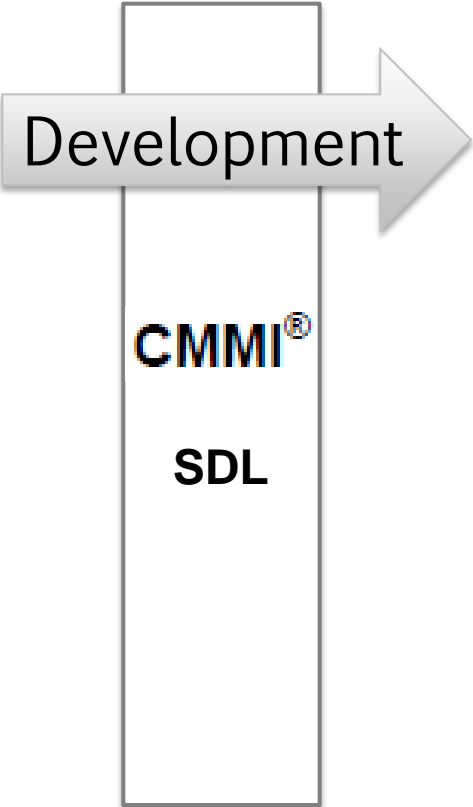
 OWASP

ScanAlert™

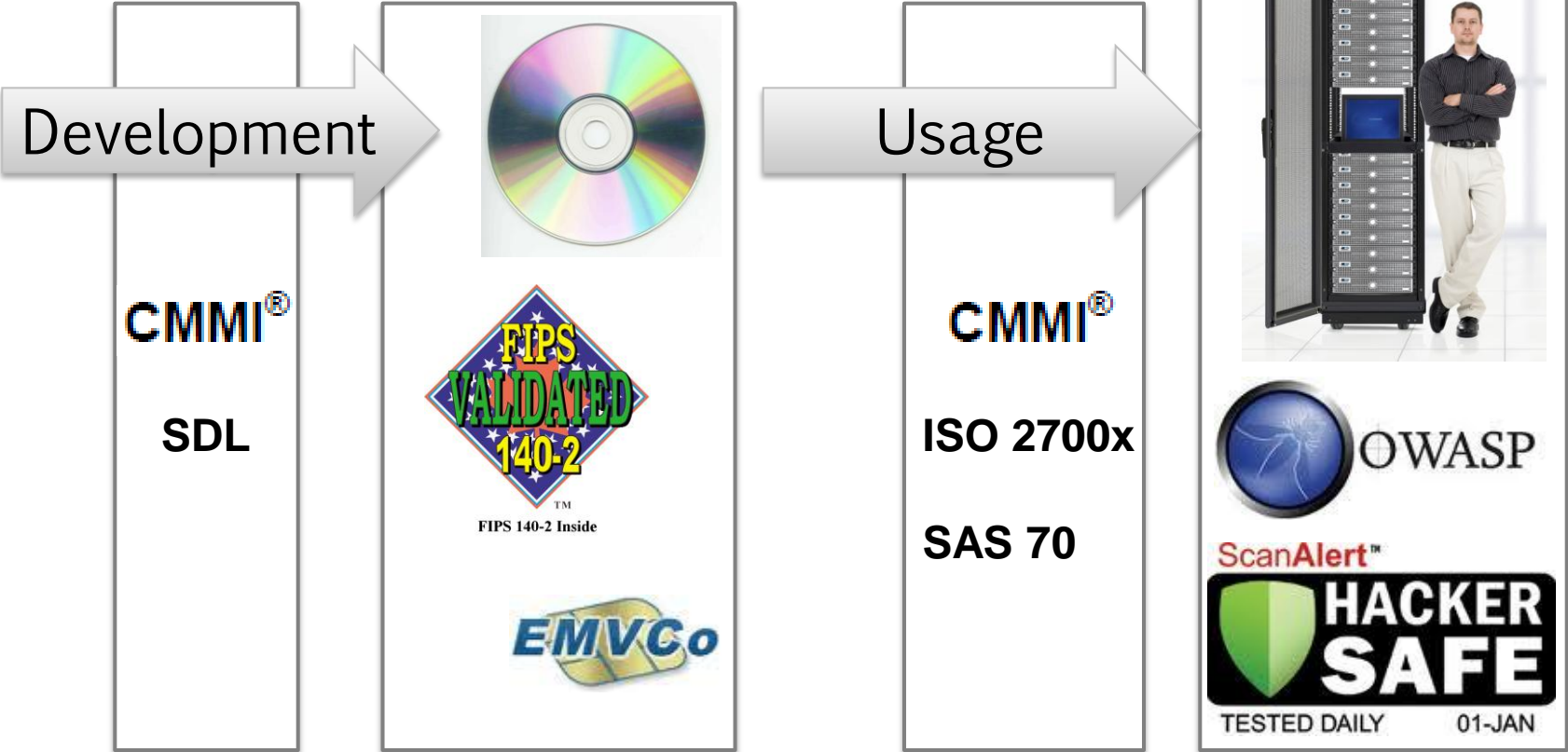
 **HACKER SAFE**

TESTED DAILY 01-JAN

Process focus

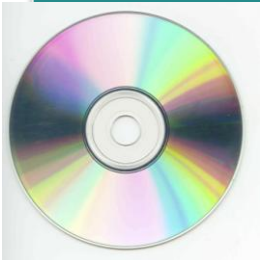


# Evaluation methodologies (single focus)



Broader focus

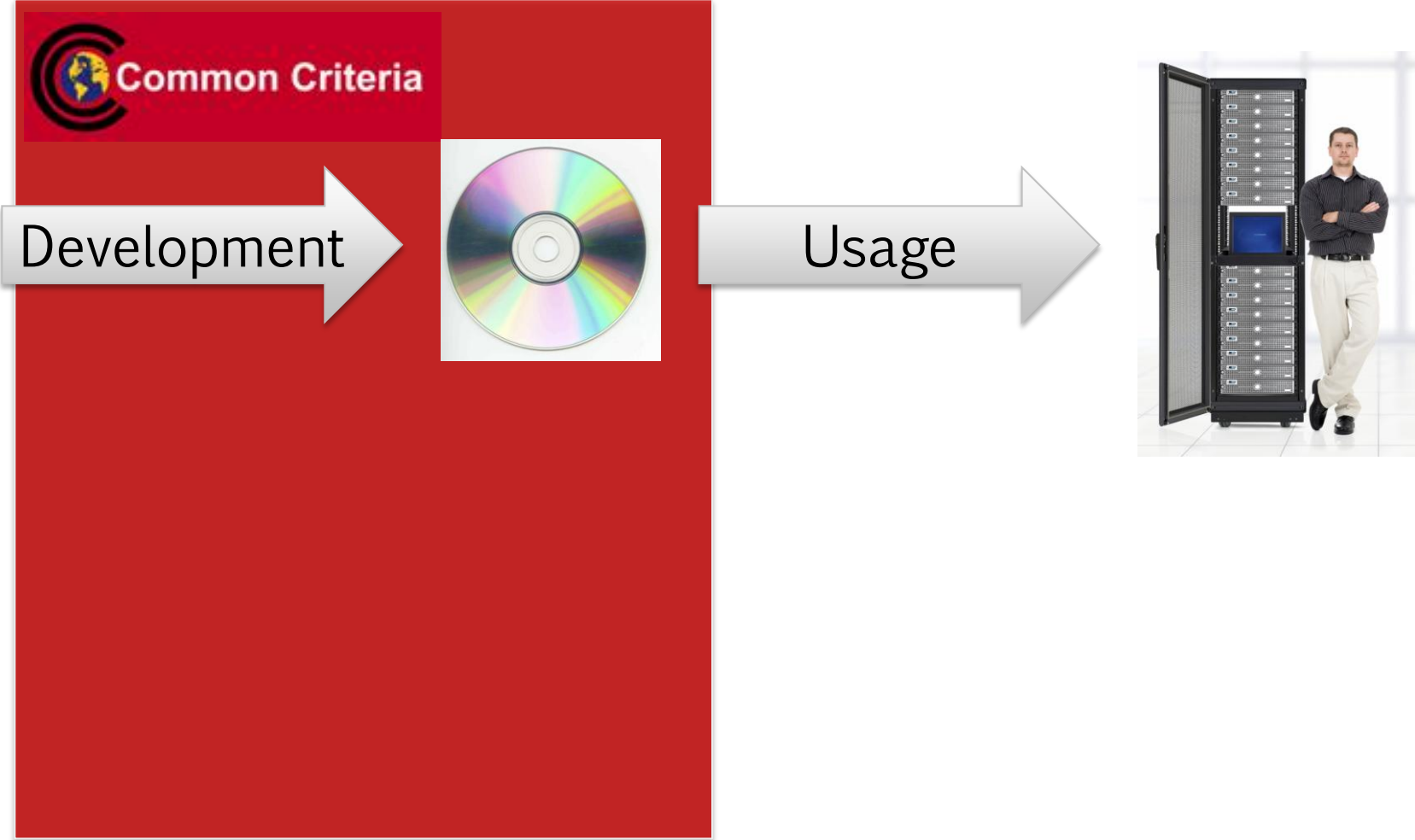
Development



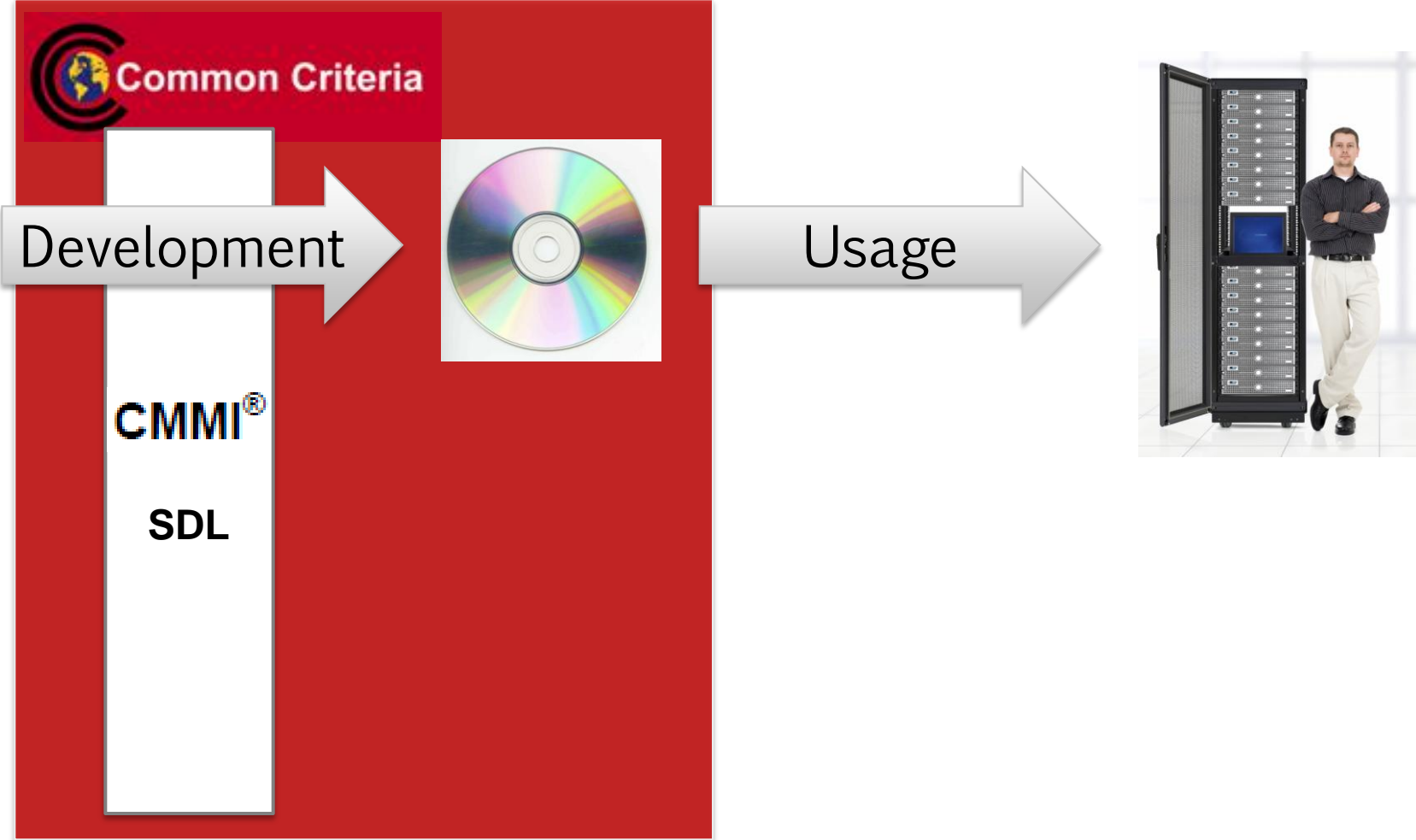
Usage



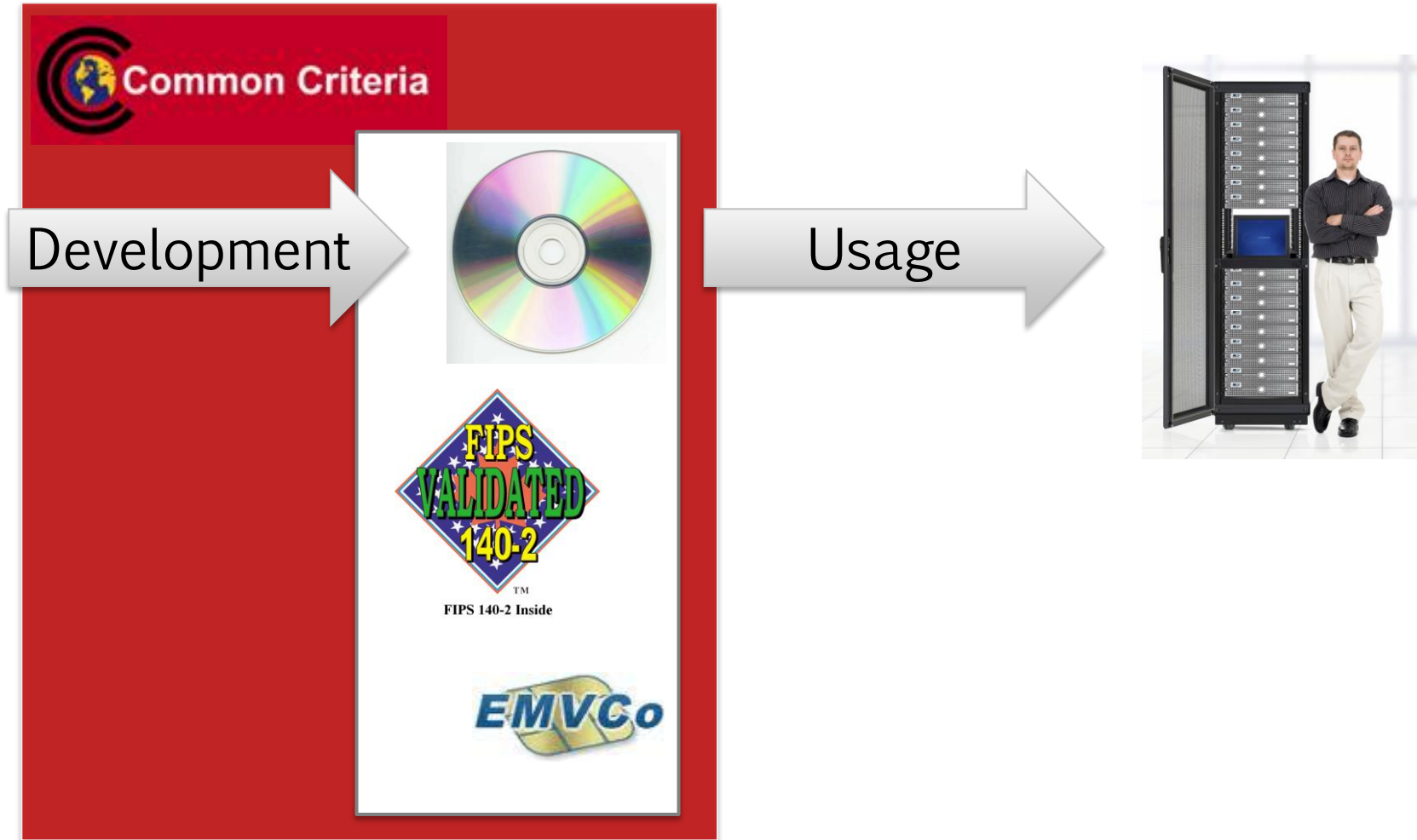
# Common Criteria



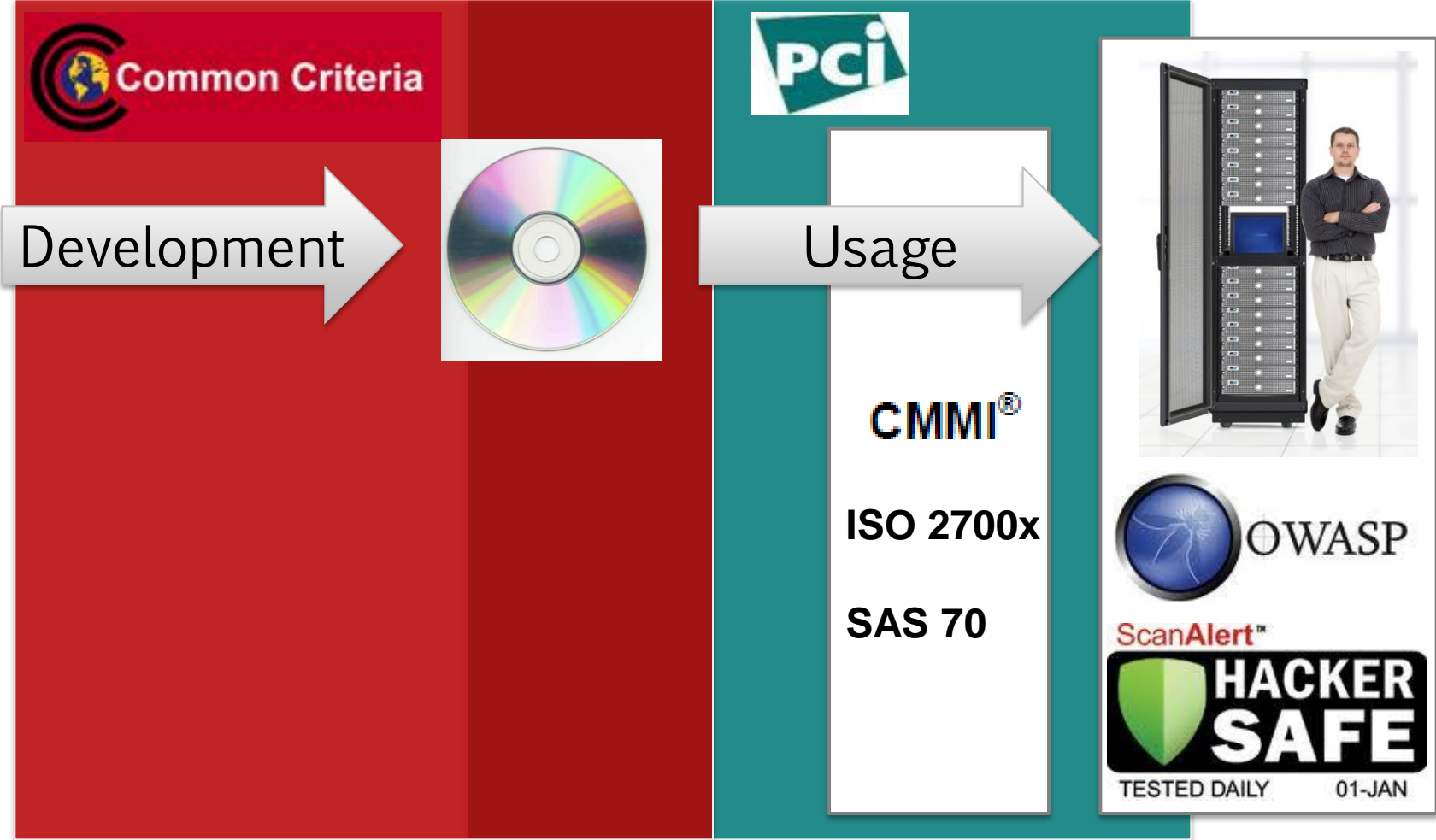
# Re-use of earlier work in the CC evaluation



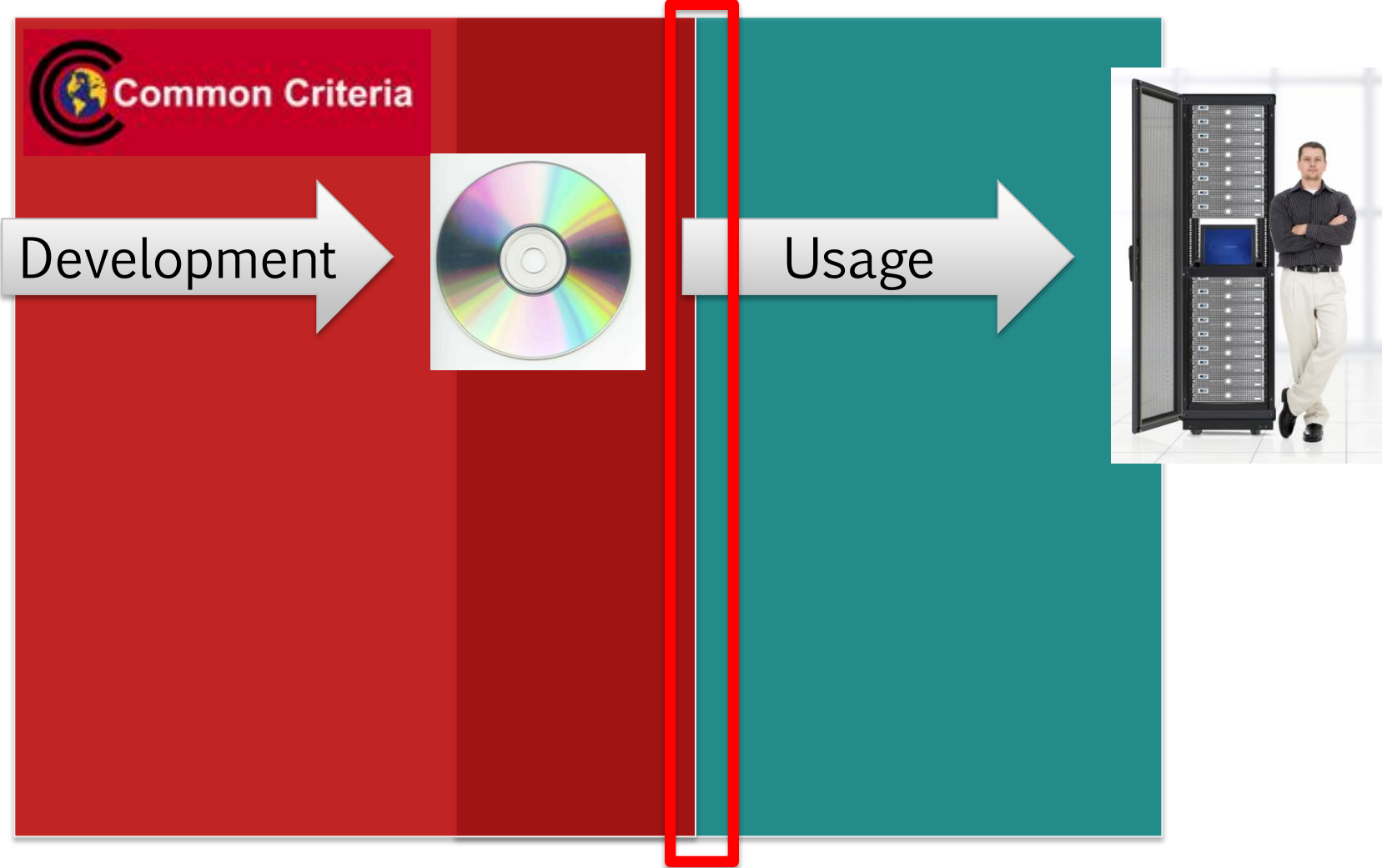
## Re-use of earlier work in the CC evaluation



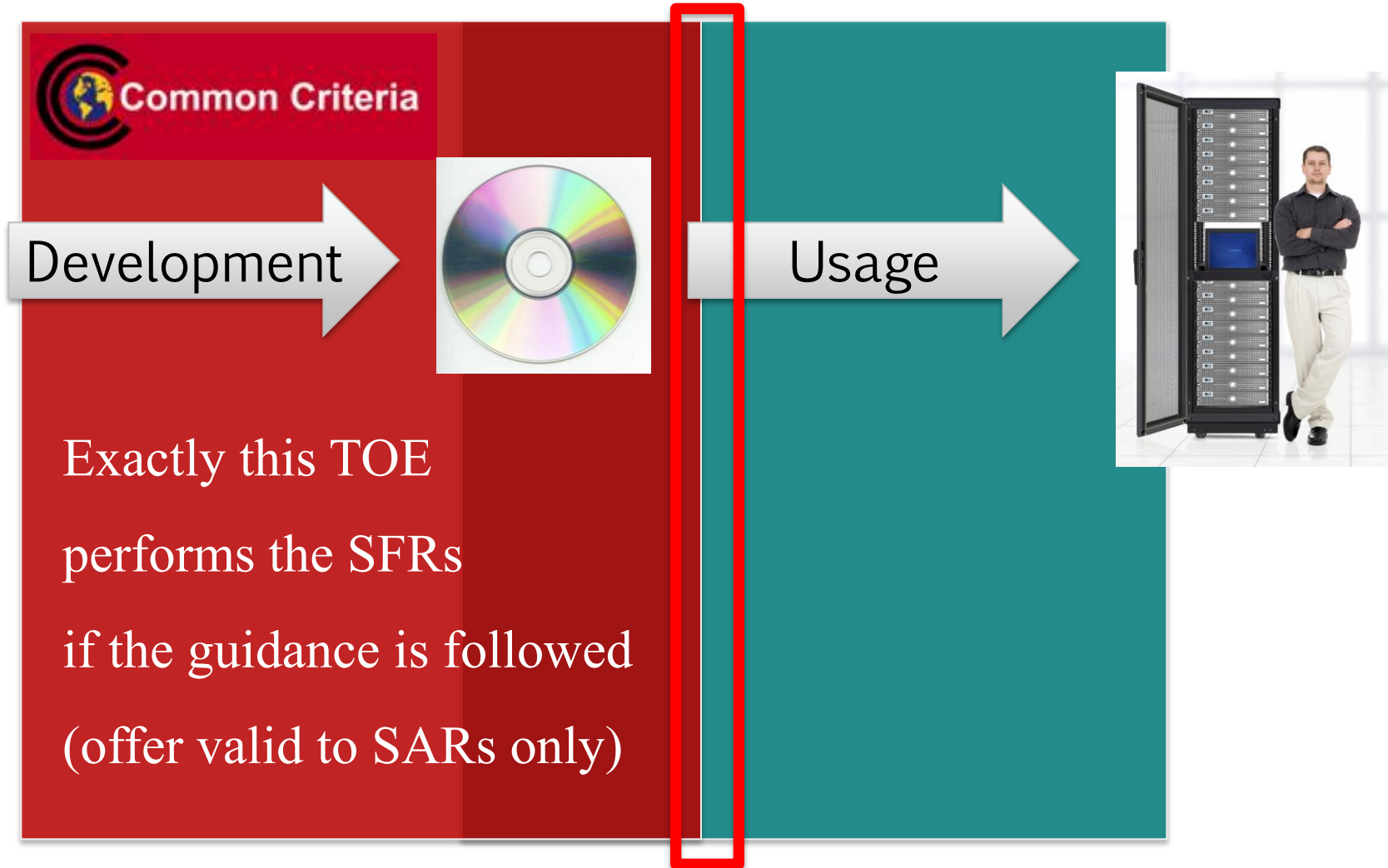
# Re-use of CC in further certification



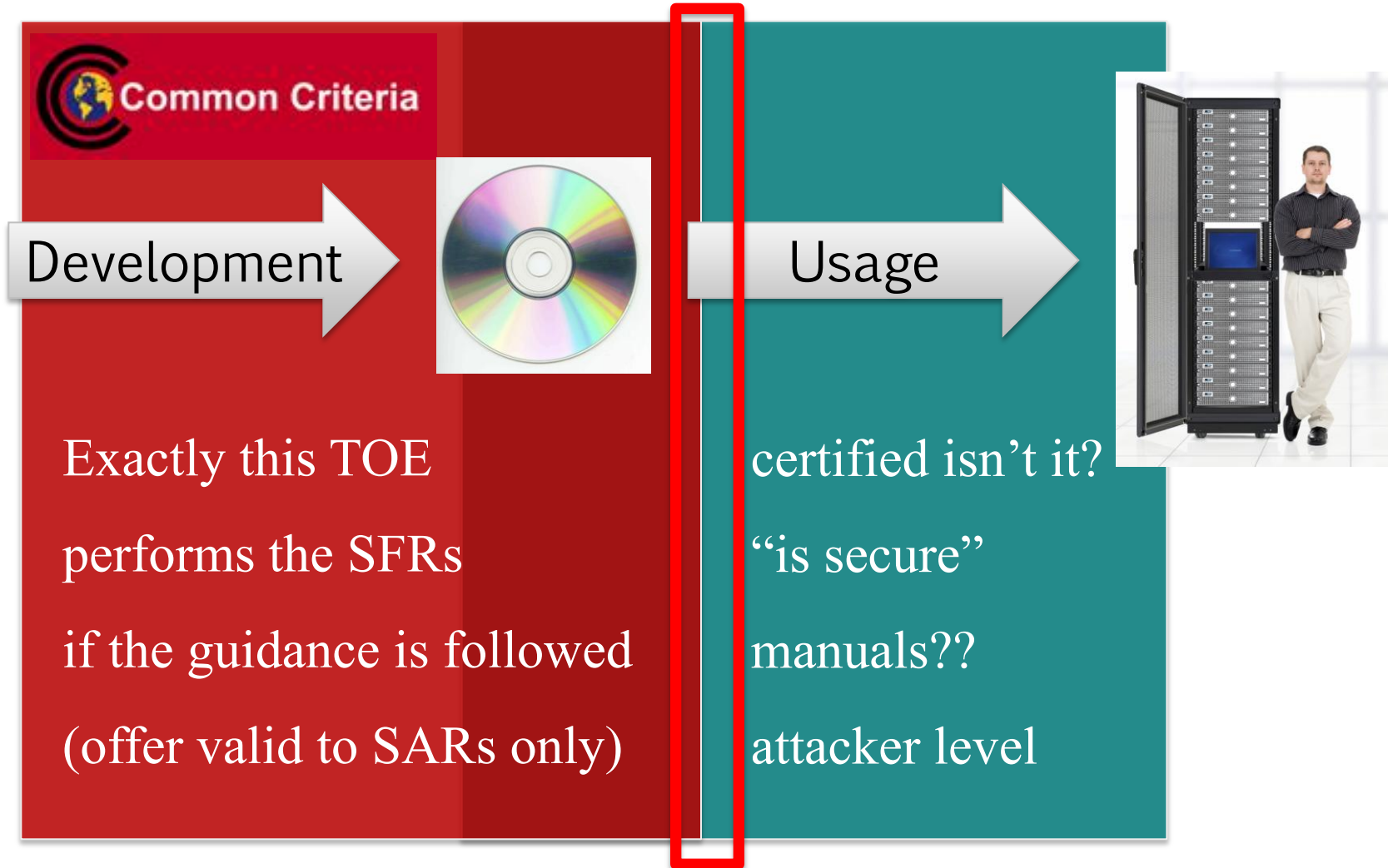
Problem area



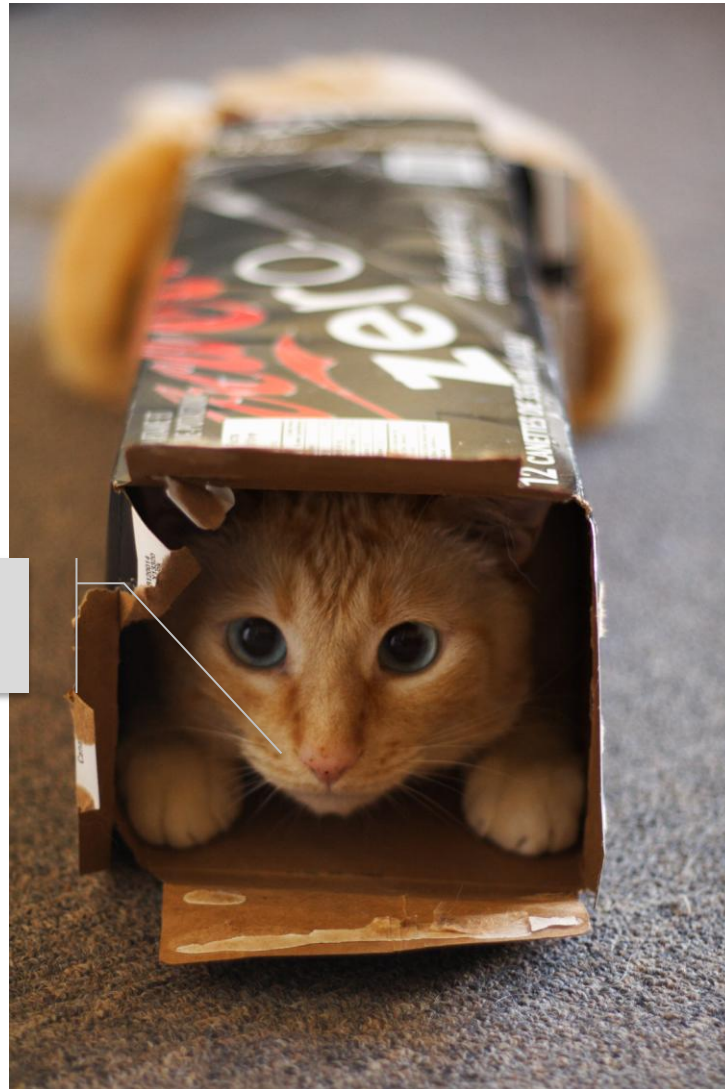
## Problem area



## Problem area



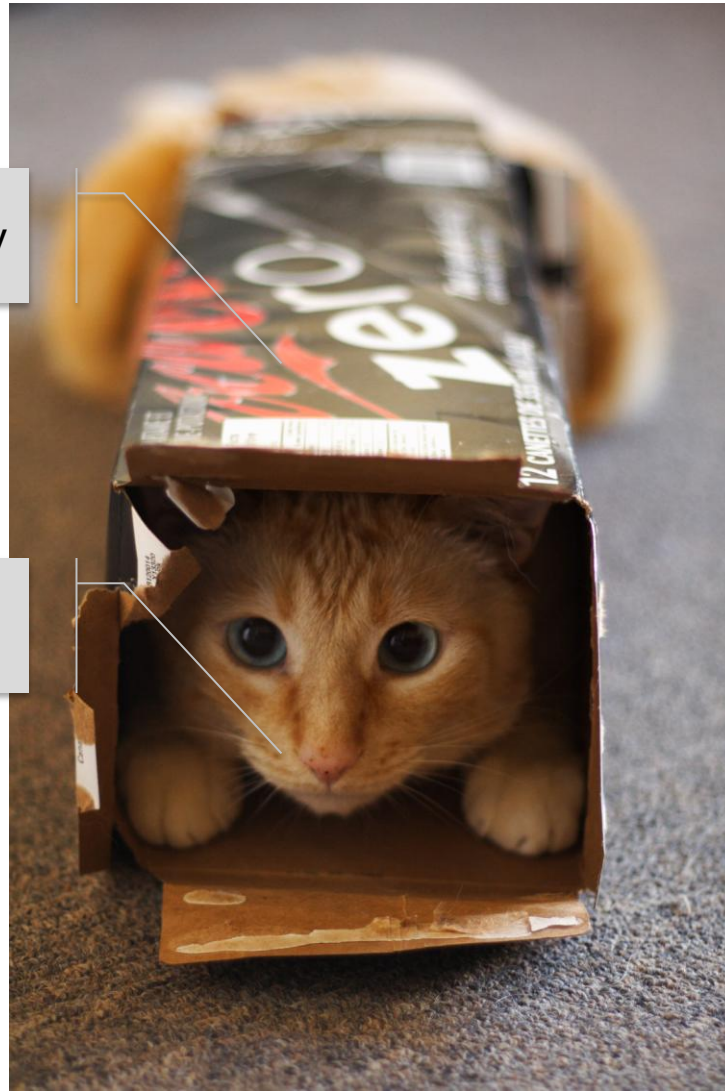
Evaluator



Slowly getting into the box  
by Greencolander  
@ flickr.com CC-BY

Evaluation methodology

Evaluator



Slowly getting into the box

by Greencolander

@ flickr.com CC-BY

Assurance limits

Assumptions



Claims

Human mistakes

Assurance limits  
AVA\_VAN.x

Assumptions  
Objectives for the  
environment  
(guidance)



Claims  
SFRs  
TOE scope

Human mistakes

Assurance limits

Assumptions



Claims

Human mistakes

# Assumptions

...everyone knows, when you make an **assumption**,  
you make an ass out of "u" and "umption".

Mitch Hennessey – The Long Kiss Goodnight



---

## Assumptions: OSeS (Windows, Linux, ...)

### A.CONNECT

All connections to peripheral devices reside within the controlled access facilities. The TOE only addresses security concerns related to the manipulation of the TOE through its authorized access points. Internal communication paths to access points such as terminals are assumed to be adequately protected.

### A.PEER

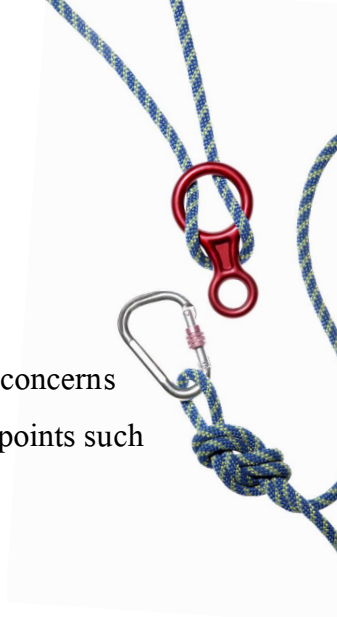
Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints. The TOE is applicable to networked or distributed environments **only if the entire network operates under the same constraints and resides within a single management domain.**

### A.COOP

**Authorized users** possess the necessary authorization to access at least some of the information managed by the TOE and are **expected to act in a cooperating manner in a benign environment.**

### A.PROTECT

The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.



## Assumptions: OSeS (Windows, Linux, ...)

### A.CONNECT

All connections to  
related to the man  
as terminals are as

Only allow access to keyboard, mouse and display

ity concerns  
ss points such

### A.PEER

Any other system  
the same security  
operates under the

No connections to the outside world

l operate under  
entire network

### A.COOP

Authorized users  
expected to act in

Users are smart and do NOT  
press “yes” on any question, run malware, ...

OE and are

### A.PROTECT

The TOE hardware  
modification.

No touching of the hardware

ical

# Assumptions: OSeS (Windows, Linux, ...)

## A.CONNECT

All connections to  
related to the man  
as terminals are as

Only

display

ity concerns  
ss points such

## A.PEER

Any other system  
the same security  
operates under the

l operate under  
entire network

## A.COOP

Authorized users  
expected to act in

p

...

OE and are

## A.PROTECT

The TOE hardware  
modification.

ical

Source:  
Protection Profiles  
CAPP / LSPP



---

Cold war government threat model

Physical protection

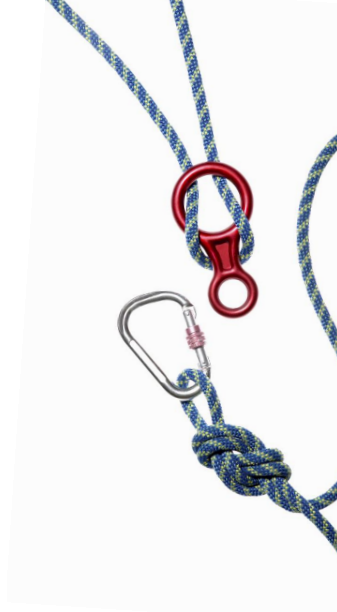
Distance to attackers

Trusted personnel


Highly compartmentalized networks



# Real world attacks: a big gap



**CVE LIST**    **COMPATIBLE PRODUCTS**    **NEWS — MARCH 11, 2010**

 **Common Vulnerabilities**  
*The Standard for Information Security*

HOME > CVE > SEARCH RESULTS

**About CVE**  
Terminology  
Documents  
FAQs

**CVE List**  
About CVE Identifiers  
Obtain a CVE Identifier  
Search CVE  
Search NVD

**CVE In Use**  
CVE Adoption  
CVE-Compatible Products  
NVD for CVE Fix Information  
More . . .


**News & Events**  
Calendar  
Free Newsletter

**Community**  
CVE Editorial Board

## Search Results

There are **2949** CVE entries or candidates that match your search.    **CVE version: 20061101**

| Name                          | Description   |
|-------------------------------|---|
| <a href="#">CVE-2010-0729</a> | A certain Red Hat patch for the Linux kernel in Red Hat Enterprise Linux (RHEL) 4 on the ia64 platform allows local users to use ptrace on an arbitrary process, and consequently gain privileges, via vectors related to a missing ptrace_check_attach call.   |
| <a href="#">CVE-2010-0727</a> | The gfs2_lock function in the Linux kernel before 2.6.34-rc1-next-20100312, and the gfs2_glock function in the Linux kernel on Red Hat Enterprise Linux (RHEL) 5 before 5.4-RC1, do not properly remove POSIX locks on files that have the sticky bit set, which allows local users to cause a denial of service (application hang) by locking a file on a (1) GFS or (2) GFS2 file system. |
| <a href="#">CVE-2010-0423</a> | gtkhtml.c in Pidgin before 2.6.6 allows remote attackers to cause a denial of service (CPU consumption and application hang) by sending a large number of messages.   |
| <a href="#">CVE-2010-0420</a> | libpurple in Finch in Pidgin before 2.6.6, when used, does not properly parse nicknames and causes remote attackers to cause a denial of service (application hang) via a long string in the SRC attribute of a (1) IMG or (2) IFRAME element.  |
| <a href="#">CVE-2010-0419</a> | The x86 emulator in KVM 83, when a guest is running, does not properly restrict writing of memory, which allows remote attackers to cause a denial of service (application crash) via a long string in the SRC attribute of a (1) IMG or (2) IFRAME element.  |

 **Common Vulnerabilities**  
*The Standard for Information Security*

HOME > CVE > SEARCH RESULTS

**About CVE**  
Terminology  
Documents  
FAQs

**CVE List**  
About CVE Identifiers  
Obtain a CVE Identifier  
Search CVE  
Search NVD

**CVE In Use**  
CVE Adoption  
CVE-Compatible Products  
NVD for CVE Fix Information  
More . . .

**News & Events**  
Calendar  
Free Newsletter

**Community**  
CVE Editorial Board  
Sponsor

## Search Results

There are **1631** CVE entries or candidates that match your search.    **CVE version: 20061101**

| Name                          | Description   |
|-------------------------------|---|
| <a href="#">CVE-2010-0925</a> | dfnetwork.dll 1.450.5.0 in CFNetwork, as used by safari.exe 531.21.10 in Apple Safari 4.0.4 on Windows, allows remote attackers to cause a denial of service (application crash) via a long string in the SRC attribute of a (1) IMG or (2) IFRAME element.   |
| <a href="#">CVE-2010-0924</a> | dfnetwork.dll 1.450.5.0 in CFNetwork, as used by safari.exe 531.21.10 in Apple Safari 4.0.3 and 4.0.4 on Windows, allows remote attackers to cause a denial of service (application crash) via a long string in the BACKGROUND attribute of a BODY element.   |
| <a href="#">CVE-2010-0917</a> | Stack-based buffer overflow in VBScript in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2, when Internet Explorer is used, might allow user-assisted remote attackers to execute arbitrary code via a long string in the fourth argument (aka helpfile argument) to the MsgBox function, leading to code execution when the F1 key is pressed, a different vulnerability than CVE-2010-0483. |
| <a href="#">CVE-2010-0719</a> | An unspecified API in Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 does not validate arguments, which allows local users to cause a denial of service (system crash) via a crafted application.   |
| <a href="#">CVE-2010-0718</a> | Buffer overflow in Microsoft Windows Media Player 9 and 11.0.5721.5145 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a  |

# Assumptions: OSeS (Windows, Linux, ...)

## A.CONNECT

All connections to  
related to the man  
as terminals are as

Only

display

ity concerns  
ss points such

Source:  
Protection Profiles  
CAPP / LSPP

## A.PEER

Any other system  
the same security  
operates under the

l operate under  
entire network

## A.COOP

Authorized users  
expected to act in

Users are smart and do NOT  
press “yes” on any question, run malware, ...

OE and are

## A.PROTECT

The TOE hardware  
modification.

No touching of the hardware

ical

---

# Assumptions: smartcards

## A.Process-Sec-IC Protection during Packaging, Finishing and Personalisation

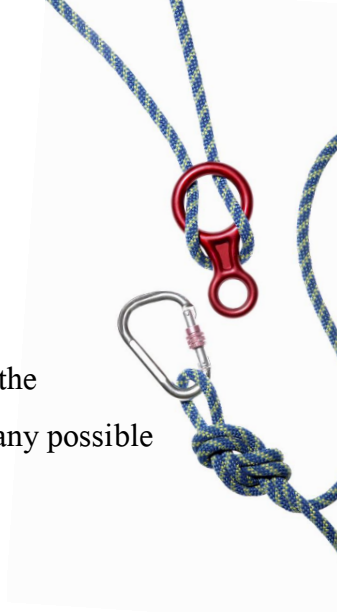
It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the endconsumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).

## A.Plat-Appl Usage of Hardware Platform

The Security IC Embedded Software is designed so that the requirements from the following documents are met: (i) TOE guidance documents (refer to the Common Criteria assurance class AGD) such as the hardware data sheet, and the hardware application notes, and (ii) findings of the TOE evaluation reports relevant for the Security IC Embedded Software as documented in the certification report

## A.Resp-Appl Treatment of User Data

All User Data are owned by Security IC Embedded Software. Therefore, it must be assumed that security relevant User Data (especially cryptographic keys) are treated by the Security IC Embedded Software as defined for its specific application context.



# Assumptions: smartcards

A.Process-Sec-IC

It is assumed that  
endconsumer to m  
copy, modification

Careful when personalizing

to the  
nt any possible

A.Plat-Appl Usage of Hardware Platform

The Security IC E  
guidance document  
application notes,  
in the certification report

Follow the programmer guidelines

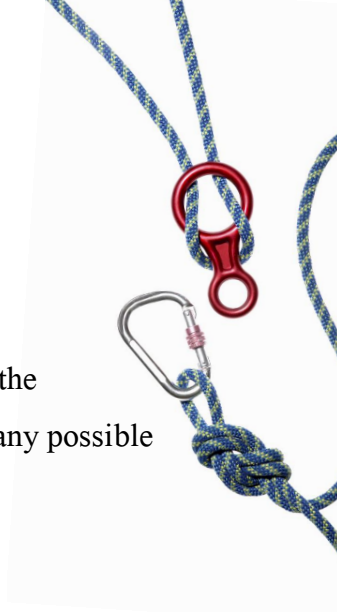
(i) TOE  
e hardware  
as documented

A.Resp-Appl Treat

All User Data are  
(especially crypto

Software: Don't output data you want to keep secret

t User Data  
cation context.



# Assumptions: smartcards

A.Process-Sec-IC

It is assumed that  
endconsumer to m  
copy, modification

Careful when personalizing

to the  
nt any possible

A.Plat-Appl Usage of Hardware Platform

The Security IC E  
guidance document  
application notes,  
in the certification report

Follow the programmer guidelines

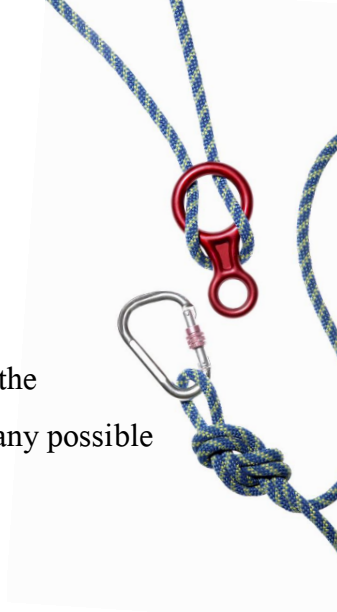
(i) TOE  
e hardware  
as documented

A.Resp-Appl Treat

All User Data are  
(especially crypto

Software: Don't output data you want to keep secret

t User Data  
cation context.



---

## Assumptions

Keep the assumptions

realistic

minimal

extremely clear

... also in the manuals!



Assurance limits

Assumptions



Claims

Human mistakes

# FIPS-140 meets USB-sticks: Claims (“SFRs” and “TOE scope”)



## Kryptografisch sicher? SySS knackt USB-Stick

*Der SySS GmbH ist es gelungen, einen Hardware-verschlüsselten USB-Stick von Kingston zu knacken, welcher über eine FIPS-Zertifizierung verfügt.*



Dipl.-Inform. Matthias Deeg  
Dipl.-Inform. Sebastian Schreiber

18. Dezember 2009



## Kryptografisch sicher? SySS knackt USB-Stick

*Der SySS GmbH ist es gelungen, einen Hardware-verschlüsselten USB-Stick von SanDisk zu knacken, welcher über eine FIPS-Zertifizierung verfügt.*



Dipl.-Inform. Matthias Deeg  
Dipl.-Inform. Sebastian Schreiber

18. Dezember 2009

---

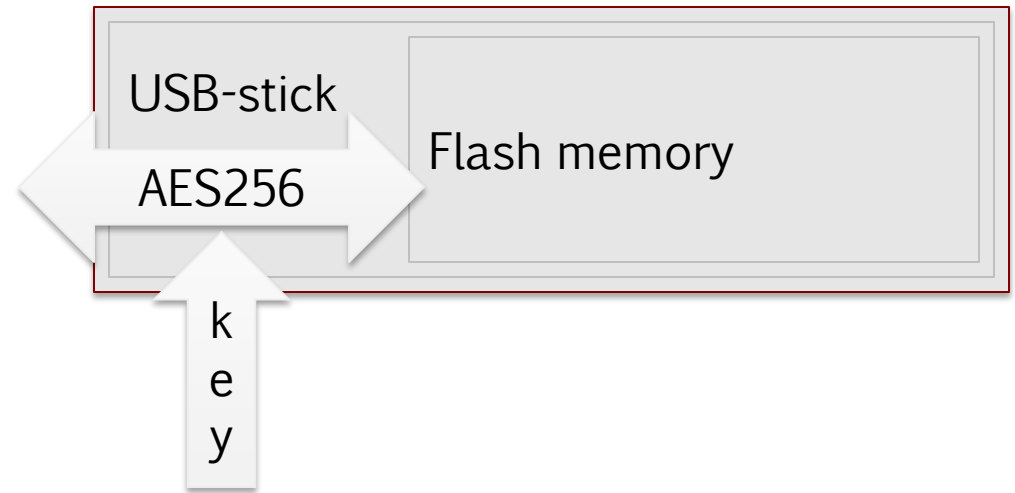
FIPS-140

Use a proper crypto algorithm  
(~FCS\_COP)

(Environment will do the rest)

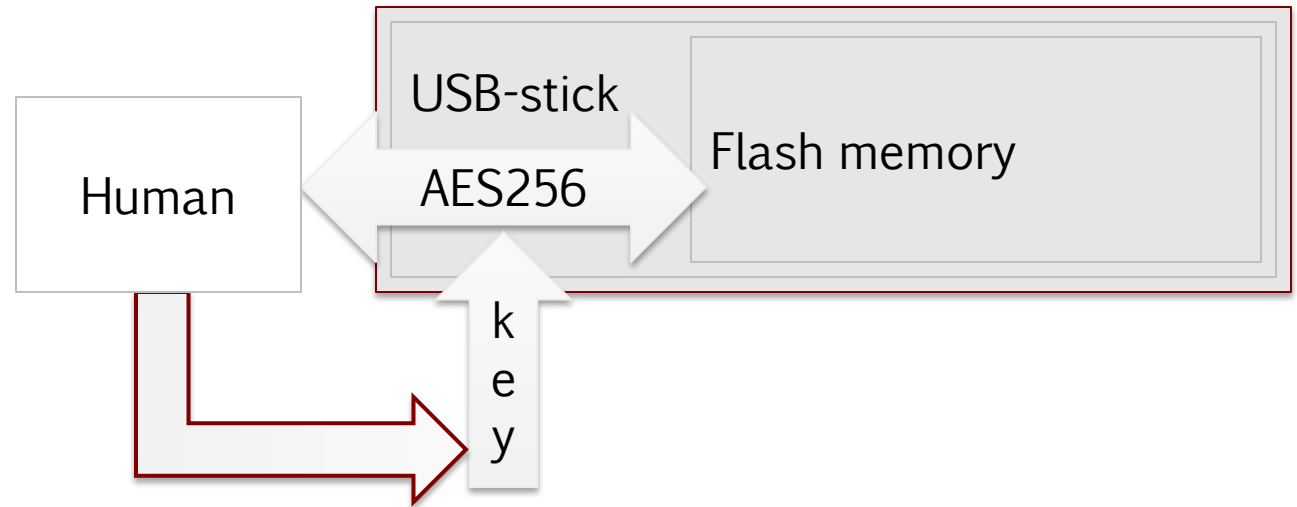


## FIPS-140 meets USB-sticks



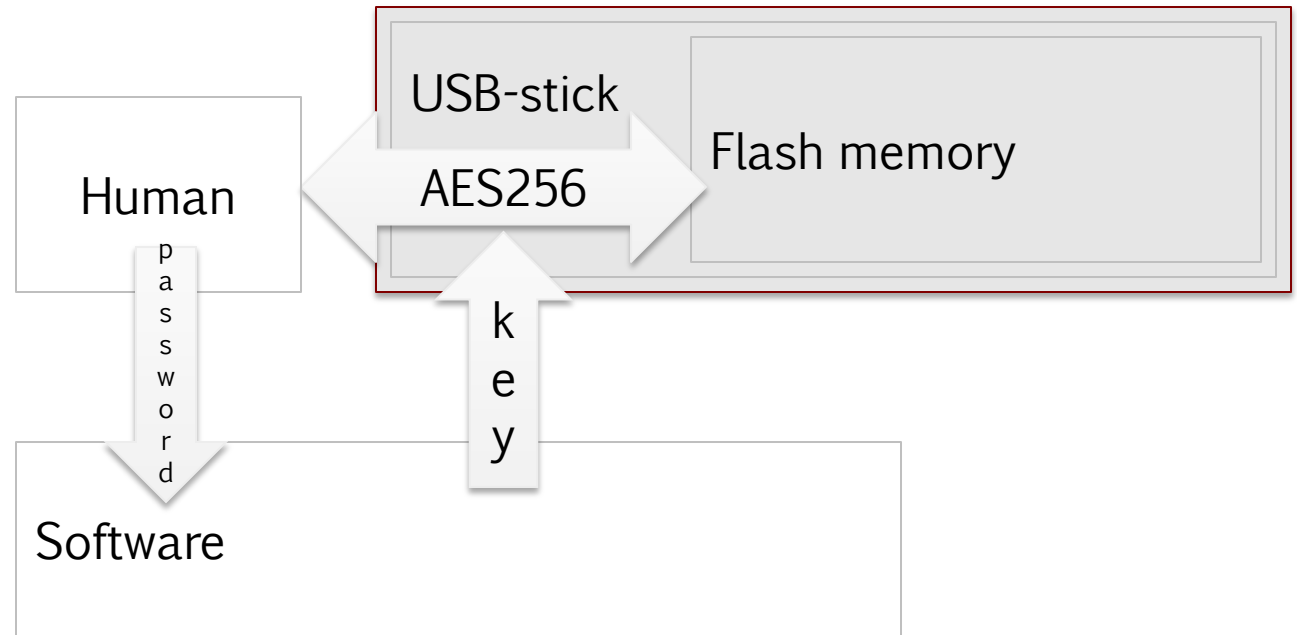
## FIPS-140 meets USB-sticks

Human inputs a good key (i.e. it is large, random and unique)



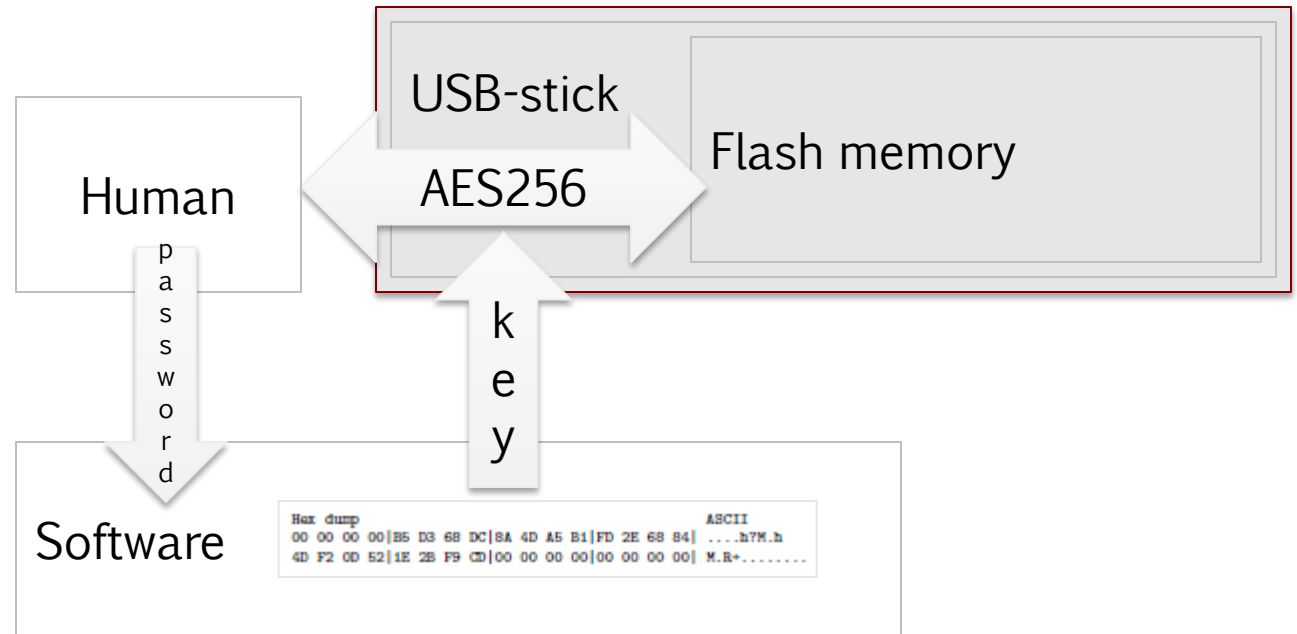
## FIPS-140 meets USB-sticks

Human inputs a good key (i.e. it is large, random and unique)



# FIPS-140 meets USB-sticks

Human inputs a good key (i.e. it is large, random and **unique**)



# FIPS-140 meets USB-sticks

## Instant hack

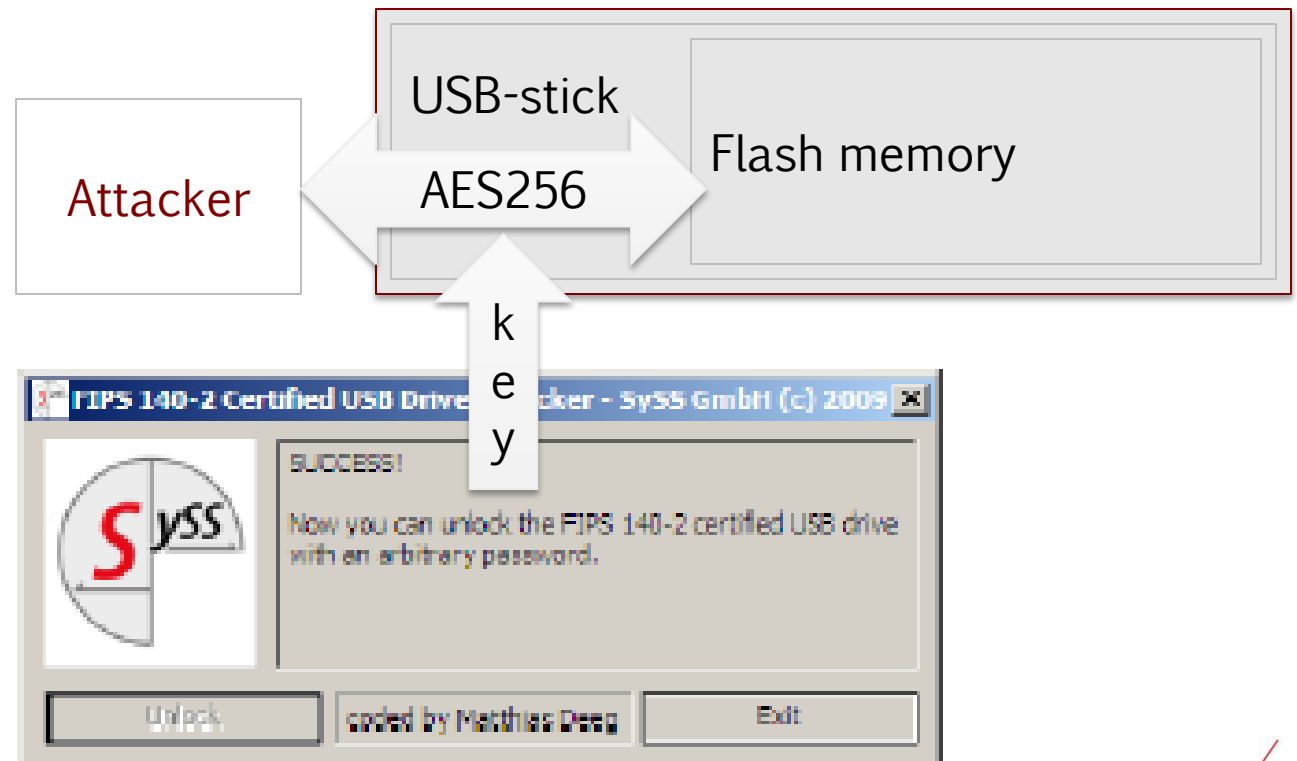


Figure 4: Proof-of-Concept software tool of the SySS GmbH

# FIPS-140 meets USB-sticks: Claims and Assumptions



## Kryptografisch sicher? SySS knackt USB-Stick

*Der SySS GmbH ist es gelungen, einen Hardware-verschlüsselten USB-Stick von Kingston zu knacken, welcher über eine FIPS-Zertifizierung verfügt.*



Dipl.-Inform. Matthias Deeg  
Dipl.-Inform. Sebastian Schreiber

18. Dezember 2009

FIPS-140 level 2  
requirements  
broken?



## Kryptografisch sicher? SySS knackt USB-Stick

*Der SySS GmbH ist es gelungen, einen Hardware-verschlüsselten USB-Stick von SanDisk zu knacken, welcher über eine FIPS-Zertifizierung verfügt.*



Dipl.-Inform. Matthias Deeg  
Dipl.-Inform. Sebastian Schreiber

18. Dezember 2009

# FIPS-140 meets USB-sticks: Claims and Assumptions



## Kryptografisch sicher? SySS knackt USB-Stick

*Der SySS GmbH ist es gelungen, einen Hardware-verschlüsselten USB-Stick von Kingston zu knacken, welcher über eine FIPS-Zertifizierung verfügt.*




Dipl.-Inform. Matthias Deeg  
Dipl.-Inform. Sebastian Schreiber

18. Dezember 2009


FIPS-140 level 2 requirements broken?

Stick still does AES with provided key (does not know key is not unique)



## Kryptografisch sicher? SySS knackt USB-Stick

*Der SySS GmbH ist es gelungen, einen Hardware-verschlüsselten USB-Stick von SanDisk zu knacken, welcher über eine FIPS-Zertifizierung verfügt.*



Dipl.-Inform. Matthias Deeg  
Dipl.-Inform. Sebastian Schreiber

18. Dezember 2009

---

Claims: TOE Scope, SFRs, real world use

Keep the claims

close to actual end-user use

clear what is not included

Keep the scope realistic

No scope tricks

Assurance limits

Assumptions



Claims

Human mistakes



Re-usable CC certifications

Clear on claims

No trickery with TOE scope

SFRs == used functionality

Realistic objectives for the environment

As limited as possible

Very clear they need to be done

Real vulnerability analysis



## Security IC Platform Protection Profile

Common Criteria Protection Profile  
BSI-CC-PP-0067  
Version 2.0

Version 1.0

15.06.2007

developed by

?????

**Atmel**  
**Infineon Technologies AG**  
**NXP Semiconductors**  
**Renesas Technology Europe Ltd.**  
**STMicroelectronics**





YOUR

WOUTER@  
YOURCREATIVESOLUTIONS.NL  
+31-6-24721971

Wouter Slegers





YOUR

WOUTER@  
YOURCREATIVESOLUTIONS.NL  
+31-6-24721971

Wouter Slegers

# Attributions



© istockphoto.com, licensed for the presentation,  
all rights reserved, no extraction allowed



“Slowly getting into the box” by Greencolander @ flickr.com CC-BY



“IMG\_4284” by babbagecabbage @ flickr.com CC-BY

Images and trademarks of respective owners, used under fair use to illustrate the discussion