

MUNI  
FI

CRCS

Centre for Research on  
Cryptography and Security

September 15, 2022

# Analyzing the security certifications landscape: Does certification help security?

Ján Jančár

Petr Švenda, Adam Janovský,  
Jiří Michalík, Stanislav Boboň





# Minerva: a group of vulnerabilities

- **ECTester**: Testing elliptic-curve cryptography implementations




# Minerva: a group of vulnerabilities



- **ECTester**: Testing elliptic-curve cryptography implementations
- Discovered a timing side-channel vulnerability in ECDSA in:
  -  libcrypt, wolfSSL, MatrixSSL, SunEC/Java, Crypto++
  -  Athena IDProtect (CC and FIPS 140 certified)



# Minerva: a group of vulnerabilities



- **ECTest**: Testing elliptic-curve cryptography implementations
- Discovered a timing side-channel vulnerability in ECDSA in:
  -  libcrypt, wolfSSL, MatrixSSL, SunEC/Java, Crypto++
  -  Athena IDProtect (CC and FIPS 140 certified)
- Responsible disclosure:
  -  Libraries
  - ✓ Analyze sources for vulnerability
  - ✓ A few emails back and forth

# Minerva: a group of vulnerabilities



- **ECTester**: Testing elliptic-curve cryptography implementations
- Discovered a timing side-channel vulnerability in ECDSA in:
  -  libcrypt, wolfSSL, MatrixSSL, SunEC/Java, Crypto++
  -  Athena IDProtect (CC and FIPS 140 certified)
- Responsible disclosure:

## Libraries

- ✓ Analyze sources for vulnerability
- ✓ A few emails back and forth

## Smartcard

- ✗ No source available, can't debug
- ✗ Athena no longer exists, sold to NXP
- ?? ?

# Vulnerability disclosure

- Notify NXP ☒

# Vulnerability disclosure

- Notify NXP ☒
- What about end users? Who are they?
  - NXP notified affected customers, but won't know about all

# Vulnerability disclosure

- Notify NXP ☒
- What about end users? Who are they?
  - NXP notified affected customers, but won't know about all
- Where is the vulnerability from? Do other implementations share it?
  - NXP pointed to the underlying ATMEL crypto library, but no details



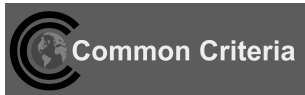
# Vulnerability disclosure



- Notify NXP ☒
- What about end users? Who are they?
  - NXP notified affected customers, but won't know about all
- Where is the vulnerability from? Do other implementations share it?
  - NXP pointed to the underlying ATMEL crypto library, but no details

**Let's look to security certifications for more info**

# Security certifications

- How to have confidence in security?
  - Without trusting vendors?
- Security certifications!
- Globally: Common Criteria standard, also EMVCo
- US: FIPS 140 standard
- Certification that product adheres to some *Security Target*
  - Vendor pays and provides materials
  - Independent lab evaluates
  - Certification body issues *Certificate* and *Certification Report*
  - Certificates released and internationally recognized
- Security target might point to a *Protection Profile* instead
  - Common set of requirements for a product class (e.g. a firewall PP)





Référence du rapport de certification	<b>ANSSI-CC-2012/23</b>
Nom du produit	<b>Athena OS755/IDProtect v6 avec application IAS-ECC sur composant AT90SC28872RCU</b>
Référence/version du produit	<ul style="list-style-type: none"> <li>- Athena IDProtect/OS755 v6 Java Card : release date 0352, release level 0005</li> <li>- Athena IAS-ECC applet : version 3, correctif F9, build 2</li> <li>- Inside Secure AT90SC28872 Microcontroller : AT58U07, révision G</li> <li>- Inside Secure Toolbox version: 00.03.11.05</li> </ul>
Conformité à un profil de protection	<p><b>[BSI-PP-0005-2002] : SSCD Type 2, version 1.04</b></p> <p><b>[BSI-PP-0006-2002] : SSCD Type 3, version 1.05</b></p>
Critères d'évaluation et version	<b>Critères Communs version 3.1 révision 3</b>
Niveau d'évaluation	<b>EAL 4 augmenté</b> <b>AVA_VAN.5</b>
Développeurs	<p><b>Athena Smartcard Solutions Inc.</b>      <b>Inside Secure S.A.</b></p> <p>1-14-16, Motoyokoyama-cho Hachioji-shi, Tokyo, 192-0063, Japan      Maxwell Building - Scottish Enterprise technology Park, East Kilbride, G75 0QR, Scotland, United Kingdom</p>
Commanditaire	<p><b>Athena Smartcard Solutions Inc.</b></p> <p>1-14-16, Motoyokoyama-cho Hachioji-shi, Tokyo, 192-0063, Japan</p>
Centre d'évaluation	<p><b>THALES (TCS – CNES)</b></p> <p>18 avenue Edouard Belin, BP11414, 31401 Toulouse Cedex 9, France</p>
Accords de reconnaissance applicables	<div>   </div> <p><b>Le produit est reconnu au niveau EAL4.</b></p>

## 1.1. ST Identification

ST title	- Athena OS755/IDProtect v6 SSCD- Athena OS755/IDProtect v6 Java Card On Inside Secure AT90SC28872RCU Microcontroller Embedding Athena IAS-ECC applet
Authors	Athena Smartcard, Inc.
General Status	Final version
ST Version Number	1.2
Date of production	March 22, 2012
TOE Reference	<p>Mask Reference: "IDProtect_AT90SC28872RCU_005"</p> <p><u>IASECC Applet</u>      <u>Athena Smartcard Solutions, Inc.</u></p> <p>AID      A000000164494153454343010101</p> <p>Version      F903</p> <p>Build      0002</p> <p>ROM Code reference:      "v0003 b0002"</p> <p>EEPROM Code Reference:      "vF903 b0002"</p> <p><u>IDProtect</u>      <u>Athena Smartcard Solutions, Inc.</u></p> <p>Release Date      0352</p> <p>Release Level      0005</p> <p>ROM Code reference:      "IDProtect_AT90SC28872RCU_005"</p> <p><u>AT90SC28872RCU</u>      <u>Inside Secure</u></p> <p>Revision      G</p> <p>Identification Number      AT58U07</p> <p>Certificate      BSI-DSZ-CC-0421-2008 [8]</p> <p><u>Ad-X</u>      <u>Inside Secure</u></p> <p>Version      00.03.11.05</p> <p>Certificate      ANSSI-CC-2009/11 [9]</p>
Common Criteria	<p>CC version 3.1</p> <p>Part 1: CCMB 2009-07-001 revision 3 [1]</p> <p>Part 2: CCMB 2009-07-002 revision 3 [2]</p> <p>Part 3: CCMB 2009-07-003 revision 3 [3]</p>
PP Claim	<p>Protection Profile — Secure Signature-Creation Device Type 2</p> <p>Version: 1.04, EAL 4+</p> <p>Wednesday, 25 July 2001</p> <p>Prepared By: ESIGN Workshop - Expert Group F</p> <p>Identification PP0005b</p> <p>Protection Profile — Secure Signature-Creation Device Type 3</p> <p>Version: 1.05, EAL 4+</p> <p>Wednesday, 25 July 2001</p> <p>Prepared By: ESIGN Workshop - Expert Group F</p> <p>Identification PP0006b</p>

[8] BSI-DSZ-CC-0421-2008 "Atmel Smartcard ICs AT90SC28872RCU / AT90SC28848RCU with Atmel Cryptographic Toolbox Version 00.03.10.00 or 00.03.13.00". CC v2.3, EAL 5+ (ALC\_DVS.2, AVA\_MSU.3, AVA\_VLA.4), compliant to BSI-PP-0002-2001 version 1.0.

[9] ANSSI-CC-2009/11 "Atmel Toolbox 00.03.11.05 on the AT90SC Family of Devices". CC v2.3, EAL 5+ (ALC\_DVS.2, AVA\_MSU.3, AVA\_VLA.4), compliant to BSI-PP-0002-2001 version 1.0.

Référence du rapport de certification	<b>ANSSI-CC-2012/23</b>
Nom du produit	<b>Athena OS755/IDProtect v6 avec application IAS-ECC sur composant AT90SC28872RCU</b>
Référence/version du produit	<ul style="list-style-type: none"> <li>- Athena IDProtect/OS755 v6 Java Card : release date 0352, release level 0005</li> <li>- Athena IAS-ECC applet : version 3, correctif F9, build 2</li> <li>- Inside Secure AT90SC28872 Microcontroller : AT58U07, révision G</li> <li>- Inside Secure Toolbox version: 00.03.11.05</li> </ul>
Conformité à un profil de protection	<p><b>[BSI-PP-0005-2002] : SSCD Type 2, version 1.04</b></p> <p><b>[BSI-PP-0006-2002] : SSCD Type 3, version 1.05</b></p>
Critères d'évaluation et version	<b>Critères Communs version 3.1 révision 3</b>
Niveau d'évaluation	<b>EAL 4 augmenté</b> <b>AVA_VAN.5</b>
Développeurs	<p><b>Athena Smartcard Solutions Inc.</b>      <b>Inside Secure S.A.</b></p> <p>1-14-16, Motoyokoyama-cho Hachioji-shi, Tokyo, 192-0063, Japan      Maxwell Building - Scottish Enterprise technology Park, East Kilbride, G75 0QR, Scotland, United Kingdom</p>
Commanditaire	<p><b>Athena Smartcard Solutions Inc.</b></p> <p>1-14-16, Motoyokoyama-cho Hachioji-shi, Tokyo, 192-0063, Japan</p>
Centre d'évaluation	<p><b>THALES (TCS – CNES)</b></p> <p>18 avenue Edouard Belin, BP11414, 31401 Toulouse Cedex 9, France</p>
Accords de reconnaissance applicables	<div>   </div> <p><b>Le produit est reconnu au niveau EAL4.</b></p>

## 1.1. ST Identification

ST title	- Athena OS755/IDProtect v6 SSCD- Athena OS755/IDProtect v6 Java Card On Inside Secure AT90SC28872RCU Microcontroller Embedding Athena IAS-ECC applet
Authors	Athena Smartcard, Inc.
General Status	Final version
ST Version Number	1.2
Date of production	March 22, 2012
TOE Reference	<p>Mask Reference: "IDProtect_AT90SC28872RCU_005"</p> <p><u>IASECC Applet</u>      <u>Athena Smartcard Solutions, Inc.</u></p> <p>AID      A000000164494153454343010101</p> <p>Version      F903</p> <p>Build      0002</p> <p>ROM Code reference:      "v0003 b0002"</p> <p>EEPROM Code Reference:      "vF903 b0002"</p> <p><u>IDProtect</u>      <u>Athena Smartcard Solutions, Inc.</u></p> <p>Release Date      0352</p> <p>Release Level      0005</p> <p>ROM Code reference:      "IDProtect_AT90SC28872RCU_005"</p> <p><u>AT90SC28872RCU</u>      <u>Inside Secure</u></p> <p>Revision      G</p> <p>Identification Number      AT58U07</p> <p>Certificate      BSI-DSZ-CC-0421-2008 [8]</p> <p><u>Ad-X</u>      <u>Inside Secure</u></p> <p>Version      00.03.11.05</p> <p>Certificate      ANSSI-CC-2009/11 [9]</p>
Common Criteria	<p>CC version 3.1</p> <p>Part 1: CCMB 2009-07-001 revision 3 [1]</p> <p>Part 2: CCMB 2009-07-002 revision 3 [2]</p> <p>Part 3: CCMB 2009-07-003 revision 3 [3]</p>
PP Claim	<p>Protection Profile — Secure Signature-Creation Device Type 2</p> <p>Version: 1.04, EAL 4+</p> <p>Wednesday, 25 July 2001</p> <p>Prepared By: ESIGN Workshop - Expert Group F</p> <p>Identification PP0005b</p> <p>Protection Profile — Secure Signature-Creation Device Type 3</p> <p>Version: 1.05, EAL 4+</p> <p>Wednesday, 25 July 2001</p> <p>Prepared By: ESIGN Workshop - Expert Group F</p> <p>Identification PP0006b</p>

[8] BSI-DSZ-CC-0421-2008 "Atmel Smartcard ICs AT90SC28872RCU / AT90SC28848RCU with Atmel Cryptographic Toolbox Version 00.03.10.00 or 00.03.13.00". CC v2.3, EAL 5+ (ALC\_DVS.2, AVA\_MSU.3, AVA\_VLA.4), compliant to BSI-PP-0002-2001 version 1.0.

[9] ANSSI-CC-2009/11 "Atmel Toolbox 00.03.11.05 on the AT90SC Family of Devices". CC v2.3, EAL 5+ (ALC\_DVS.2, AVA\_MSU.3, AVA\_VLA.4), compliant to BSI-PP-0002-2001 version 1.0.

<b>ST title</b>	<b>- Athena OS755/IDProtect v6 SSCD- Athena OS755/IDProtect v6 Java Card On Inside Secure AT90SC28872RCU Microcontroller Embedding Athena IAS-ECC applet</b>
<b>Authors</b>	Athena Smartcard, Inc.
<b>General Status</b>	Final version
<b>ST Version Number</b>	1.2
<b>Date of production</b>	March 22, 2012
<b>TOE Reference</b>	<p>Mask Reference: "IDProtect_AT90SC28872RCU_005"  <u>IASECC Applet</u>      <u>Athena Smartcard Solutions, Inc.</u></p> <p>AID      A000000164494153454343010101  Version      F903  Build      0002  ROM Code reference:      "v0003 b0002"  EEPROM Code Reference:      "vF903 b0002"</p> <p><u>IDProtect</u>      <u>Athena Smartcard Solutions, Inc.</u></p> <p>Release Date      0352  Release Level      0005  ROM Code reference:      "IDProtect_AT90SC28872RCU_005"</p> <p><u>AT90SC28872RCU</u>      <u>Inside Secure</u></p> <p>Revision      G  Identification Number      AT58U07  Certificate      BSI-DSZ-CC-0421-2008 [8]</p> <p><u>Ad-X</u>      <u>Inside Secure</u></p> <p>Version      00.03.11.05  Certificate      ANSSI-CC-2009/11 [9]</p>
<b>Common Criteria</b>	<p>CC version 3.1</p> <p>Part 1: CCMB 2009-07-001 revision 3 [1]  Part 2: CCMB 2009-07-002 revision 3 [2]  Part 3: CCMB 2009-07-003 revision 3 [3]</p>
<b>PP Claim</b>	<p>Protection Profile — Secure Signature-Creation Device Type 2  Version: 1.04, EAL 4+  Wednesday, 25 July 2001  Prepared By: ESIGN Workshop - Expert Group F  Identification PP0005b</p> <p>Protection Profile — Secure Signature-Creation Device Type 3  Version: 1.05, EAL 4+  Wednesday, 25 July 2001  Prepared By: ESIGN Workshop - Expert Group F  Identification PP0006b</p>

[8] BSI-DSZ-CC-0421-2008 "Atmel Smartcard ICs AT90SC28872RCU / AT90SC28848RCU with Atmel Cryptographic Toolbox Version 00.03.10.00 or 00.03.13.00". CC v2.3, EAL 5+ (ALC\_DVS.2, AVA\_MSU.3, AVA\_VLA.4), compliant to BSI-PP-0002-2001 version 1.0.

[9] ANSSI-CC-2009/11 "Atmel Toolbox 00.03.11.05 on the AT90SC Family of Devices". CC v2.3, EAL 5+ (ALC DVS.2 AVA MSU.3 AVA VLA.4), compliant to BSI-PP-0002-2001 version 1.0.



Référence du rapport de certification	
<b>ANSSI-CC-2012/23</b>	
Nom du produit	
<b>Athena OS755/IDProtect v6 avec application IAS-ECC sur composant AT90SC28872RCU</b>	
Référence/version du produit	
<ul style="list-style-type: none"> <li>- Athena IDProtect/OS755 v6 Java Card : release date 0352, release level 0005</li> <li>- Athena IAS-ECC applet : version 3, correctif F9, build 2</li> <li>- Inside Secure AT90SC28872 Microcontroller : AT58U07, révision G</li> <li>- Inside Secure Toolbox version: 00.03.11.05</li> </ul>	
Conformité à un profil de protection	
<b>[BSI-PP-0005-2002] : SSCD Type 2, version 1.04</b> <b>[BSI-PP-0006-2002] : SSCD Type 3, version 1.05</b>	
Critères d'évaluation et version	
<b>Critères Communs version 3.1 révision 3</b>	
Niveau d'évaluation	
<b>EAL 4 augmenté</b> <b>AVA_VAN.5</b>	
Développeurs	
<b>Athena Smartcard Solutions Inc.</b> 1-14-16, Motoyokoyama-cho Hachioji-shi, Tokyo, 192-0063, Japan	<b>Inside Secure S.A.</b> Maxwell Building - Scottish Enterprise technology Park, East Kilbride, G75 0QR, Scotland, United Kingdom
Commanditaire	
<b>Athena Smartcard Solutions Inc.</b> 1-14-16, Motoyokoyama-cho Hachioji-shi, Tokyo, 192-0063, Japan	
Centre d'évaluation	
<b>THALES (TCS – CNES)</b> 18 avenue Edouard Belin, BP11414, 31401 Toulouse Cedex 9, France	
Accords de reconnaissance applicables	
Le produit est reconnu au niveau EAL4.	

## 1.1. ST Identification

ST title	- Athena OS755/IDProtect v6 SSCD- Athena OS755/IDProtect v6 Java Card On Inside Secure AT90SC28872RCU Microcontroller Embedding Athena IAS-ECC applet
Authors	Athena Smartcard, Inc.
General Status	Final version
ST Version Number	1.2
Date of production	March 22, 2012
TOE Reference	Mask Reference: "IDProtect_AT90SC28872RCU_005" IASECC Applet Athena Smartcard Solutions, Inc. AID A000000164494153454343010101 Version F903 Build 0002 ROM Code reference: "v0003 b0002" EEPROM Code Reference: "vF903 b0002" IDProtect Athena Smartcard Solutions, Inc. Release Date 0352 Release Level 0005 ROM Code reference: "IDProtect_AT90SC28872RCU_005" AT90SC28872RCU Inside Secure Revision G Identification Number AT58U07 Certificate BSI-DSZ-CC-0421-2008 [8] Ad-X Inside Secure Version 00.03.11.05 Certificate ANSSI-CC-2009/11 [9]
Common Criteria	CC version 3.1 Part 1: CCMB 2009-07-001 revision 3 [1] Part 2: CCMB 2009-07-002 revision 3 [2] Part 3: CCMB 2009-07-003 revision 3 [3]
PP Claim	Protection Profile — Secure Signature-Creation Device Type 2 Version: 1.04, EAL 4+ Wednesday, 25 July 2001 Prepared By: ESIGN Workshop - Expert Group F Identification PP0005b Protection Profile — Secure Signature-Creation Device Type 3 Version: 1.05, EAL 4+ Wednesday, 25 July 2001 Prepared By: ESIGN Workshop - Expert Group F Identification PP0006b

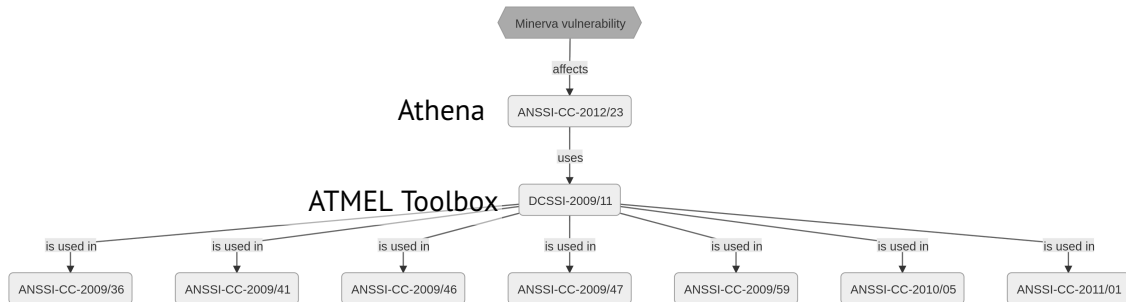
[8] BSI-DSZ-CC-0421-2008 "Atmel Smartcard ICs AT90SC28872RCU / AT90SC28848RCU with Atmel Cryptographic Toolbox Version 00.03.10.00 or 00.03.13.00". CC v2.3, EAL 5+ (ALC\_DVS.2, AVA\_MSU.3, AVA\_VLA.4), compliant to BSI-PP-0002-2001 version 1.0.

[9] ANSSI-CC-2009/11 "Atmel Toolbox 00.03.11.05 on the AT90SC Family of Devices". CC v2.3, EAL 5+ (ALC\_DVS.2, AVA\_MSU.3, AVA\_VLA.4), compliant to BSI-PP-0002-2001 version 1.0.

<b>ST title</b>	<b>- Athena OS755/IDProtect v6 SSCD- Athena OS755/IDProtect v6 Java Card On Inside Secure AT90SC28872RCU Microcontroller Embedding Athena IAS-ECC applet</b>
<b>Authors</b>	Athena Smartcard, Inc.
<b>General Status</b>	Final version
<b>ST Version Number</b>	1.2
<b>Date of production</b>	March 22, 2012
<b>TOE Reference</b>	Mask Reference: "IDProtect_AT90SC28872RCU_005" <u>IASECC Applet</u> <u>Athena Smartcard Solutions, Inc.</u> AID      A000000164494153454343010101 Version      F903 Build      0002 ROM Code reference:      "v0003 b0002" EEPROM Code Reference:      "vF903 b0002" <u>IDProtect</u> <u>Athena Smartcard Solutions, Inc.</u> Release Date      0352 Release Level      0005 ROM Code reference:      "IDProtect_AT90SC28872RCU_005" <u>AT90SC28872RCU</u> <u>Inside Secure</u> Revision      G Identification Number      AT58U07 Certificate      BSI-DSZ-CC-0421-2008 [8] <u>Ad-X</u> <u>Inside Secure</u> Version      00.03.11.05 Certificate      ANSSI-CC-2009/11 [9]
<b>Common Criteria</b>	CC version 3.1 Part 1: CCMB 2009-07-001 revision 3 [1] Part 2: CCMB 2009-07-002 revision 3 [2] Part 3: CCMB 2009-07-003 revision 3 [3]
<b>PP Claim</b>	Protection Profile — Secure Signature-Creation Device Type 2 Version: 1.04, EAL 4+ Wednesday, 25 July 2001 Prepared By: ESIGN Workshop - Expert Group F Identification PP0005b  Protection Profile — Secure Signature-Creation Device Type 3 Version: 1.05, EAL 4+ Wednesday, 25 July 2001 Prepared By: ESIGN Workshop - Expert Group F Identification PP0006b

[9] ANSSI-CC-2009/11 "Atmel Toolbox 00.03.11.05 on the AT90SC Family of Devices". CC v2.3, EAL 5+ (ALC DVS.2,AVA MSU.3,AVA VLA.4), compliant to BSI-PP-0002-2001 version 1.0.

# Back to Minerva: CC

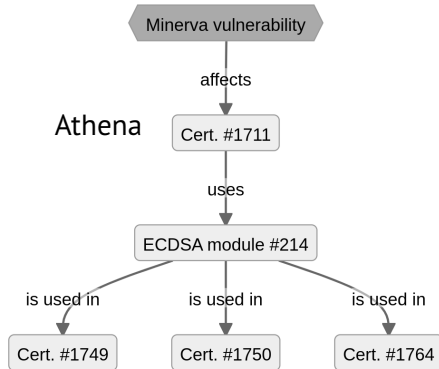


Note

\* The **Fast** functions of M10.3, M10.4, M10.5, M10.7, M10.8, M10.9, **do not** offer any DPA/SPA protection and **must** not be used for secure data.



# Back to Minerva: FIPS 140



# Manual labor?

## Volume

- CC: 5k certificates
- FIPS 140: 4k certificates

## Issues

- **No common format,  
written by people for people**
- No search
- Typos
- PDFs that are not PDFs
- Errors in data
- Scanned documents



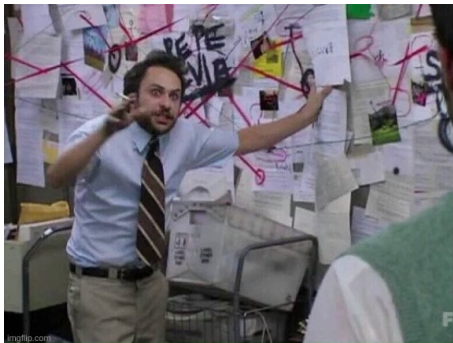
# Manual labor?

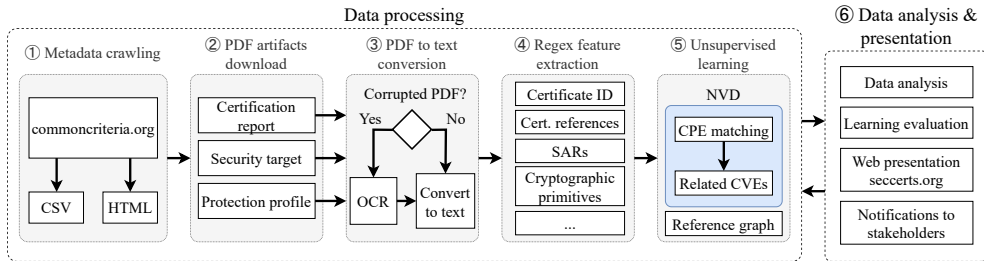
## Volume

- CC: 5k certificates
- FIPS 140: 4k certificates

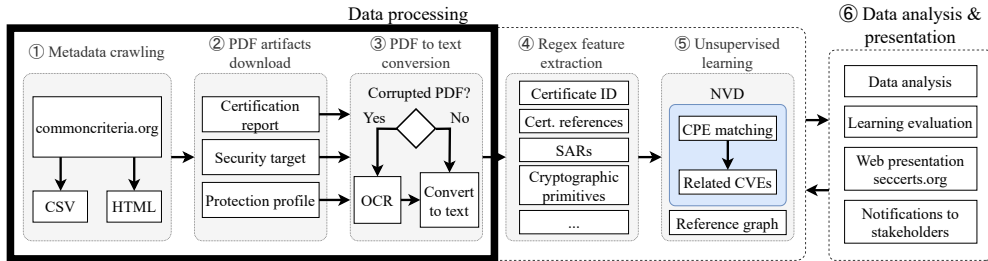
## Issues

- **No common format,  
written by people for people**
- No search
- Typos
- PDFs that are not PDFs
- Errors in data
- Scanned documents

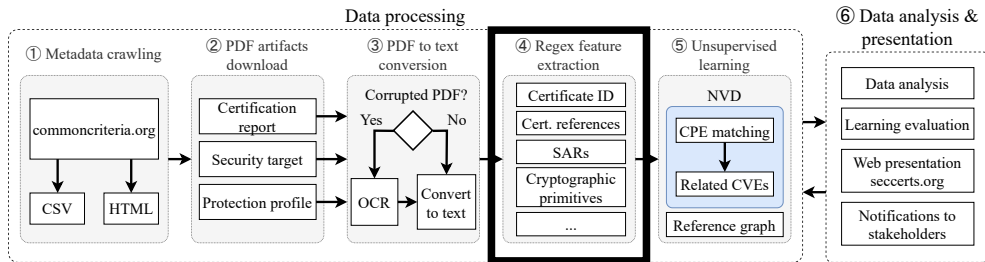




# Automate!



# Feature extraction



# Feature extraction

- Certification ID
- References to other certificates
- Security assurance requirements
- Security functional requirements
- Security levels
- References to standards (ISO/IEC, ...)
- Javacard platform, API constants
- Cryptographic algorithms
- Elliptic curves
- Cryptographic libraries
- Defenses
- ...

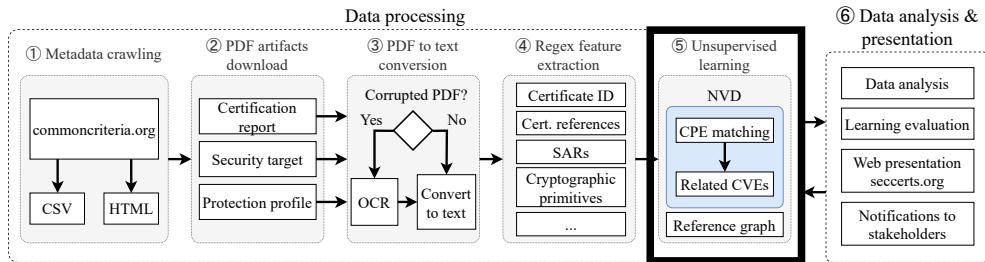
## Limitations

- No context

## Future work

- Try Natural Language Processing

# Mapping of vulnerabilities





# Mapping of vulnerabilities

- **Question:** Which certified products are affected by a given vulnerability?
- **Solution:** Map CVEs to certificates via their CPEs from NVD
  - *Common Vulnerabilities and Exposures*
  - *Common Platform Enumeration*
  - *NIST's Vulnerability Database*

# Mapping of vulnerabilities

- **Question:** Which certified products are affected by a given vulnerability?
- **Solution:** Map CVEs to certificates via their CPEs from NVD
  - *Common Vulnerabilities and Exposures*
  - *Common Platform Enumeration*
  - *NIST's Vulnerability Database*
- Example CPE:  
`cpe:2.3:a:infineon:rsa_library:1.02.013:*:*:*:*:*:*`

# Mapping of vulnerabilities

- **Question:** Which certified products are affected by a given vulnerability?
- **Solution:** Map CVEs to certificates via their CPEs from NVD
  - *Common Vulnerabilities and Exposures*
  - *Common Platform Enumeration*
  - *NIST's Vulnerability Database*
- Example CPE:  
`cpe:2.3:a:infineon:rsa_library:1.02.013:*:*:*:*:*:*`
- Example certificate name:  
Infineon Technologies Security Controller M7793 A12 and G12 with optional RSA2048/4096 v1.02.010 or v1.02.013, EC v1.02.010 or v1.02.013 and Toolbox v1.02.010 or v1.02.013 libraries and with specific IC-dedicated software

# Mapping of vulnerabilities

- **Question:** Which certified products are affected by a given vulnerability?
- **Solution:** Map CVEs to certificates via their CPEs from NVD
  - *Common Vulnerabilities and Exposures*
  - *Common Platform Enumeration*
  - *NIST's Vulnerability Database*
- Example CPE:  
`cpe:2.3:a:infineon:rsa_library:1.02.013:*:*:*:*:*:*`
- Example certificate name:  
**Infineon** Technologies Security Controller M7793 A12 and G12 with optional RSA2048/4096 v1.02.010 or v1.02.013, EC v1.02.010 or v1.02.013 and Toolbox v1.02.010 or v1.02.013 libraries and with specific IC-dedicated software

# Mapping of vulnerabilities

- **Question:** Which certified products are affected by a given vulnerability?
- **Solution:** Map CVEs to certificates via their CPEs from NVD
  - *Common Vulnerabilities and Exposures*
  - *Common Platform Enumeration*
  - *NIST's Vulnerability Database*
- Example CPE:  
`cpe:2.3:a:infineon:rsa_library:1.02.013:*:*:*:*:*:*`
- Example certificate name:  
**Infineon** Technologies Security Controller M7793 A12 and G12 with optional **RSA2048/4096** v1.02.010 or v1.02.013, EC v1.02.010 or v1.02.013 and Toolbox v1.02.010 or v1.02.013 libraries and with specific IC-dedicated software

# Mapping of vulnerabilities

- **Question:** Which certified products are affected by a given vulnerability?
- **Solution:** Map CVEs to certificates via their CPEs from NVD
  - *Common Vulnerabilities and Exposures*
  - *Common Platform Enumeration*
  - *NIST's Vulnerability Database*
- Example CPE:  
`cpe:2.3:a:infineon:rsa_library:1.02.013:*:*:*:*:*:*`
- Example certificate name:  
**Infineon** Technologies Security Controller M7793 A12 and G12 with optional **RSA2048/4096** v1.02.010 or v1.02.013, EC v1.02.010 or v1.02.013 and Toolbox v1.02.010 or v1.02.013 **libraries** and with specific IC-dedicated software

# Mapping of vulnerabilities

- **Question:** Which certified products are affected by a given vulnerability?
- **Solution:** Map CVEs to certificates via their CPEs from NVD
  - *Common Vulnerabilities and Exposures*
  - *Common Platform Enumeration*
  - *NIST's Vulnerability Database*
- Example CPE:  
`cpe:2.3:a:infineon:rsa_library:1.02.013:*:*:*:*:*:*`
- Example certificate name:  
**Infineon** Technologies Security Controller M7793 A12 and G12 with optional **RSA2048/4096** v1.02.010 or **v1.02.013**, EC v1.02.010 or v1.02.013 and Toolbox v1.02.010 or v1.02.013 **libraries** and with specific IC-dedicated software

# Mapping of vulnerabilities

## Evaluation

- 🛡️ Vulnerabilities: 615 out of 5107 CC certificates
- Manually evaluated correctness ~ 89%
- Limitations:
  - CPE <-> Name match only
  - No configuration details
  - Noisy data

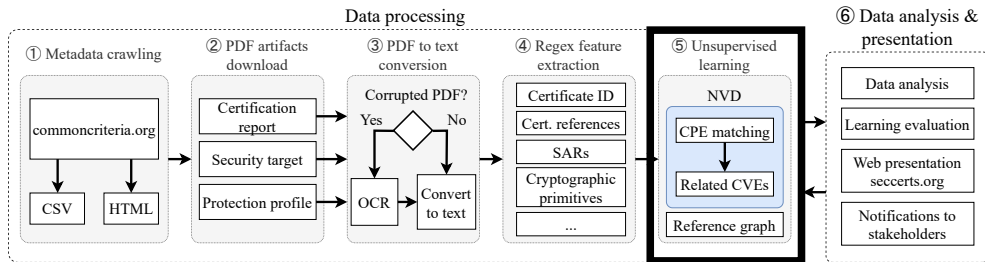


# Mapping of vulnerabilities

## Security

- **Question:** Do certifications help security?
- **Easier question:** Do higher assurance levels lead to less (severe) vulnerabilities?
- **Easier question:** Do higher assurance levels correlate with less (severe) vulns?
- Luckily they do (slightly):
  - $\rho = -0.12$  with number of vulnerabilities
  - $\rho = -0.15$  with severity of vulnerabilities

# Certificate references



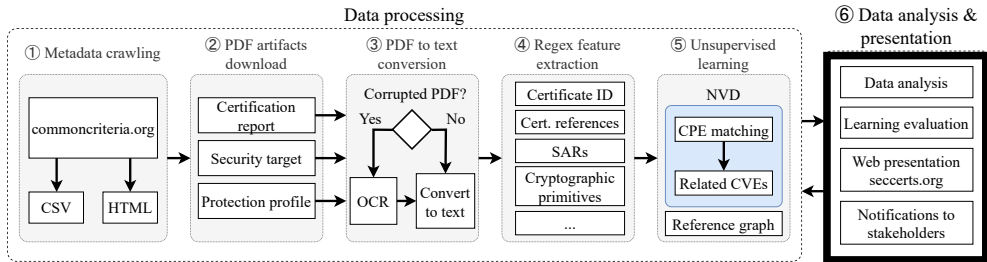
# Certificate references

- **Question:** What (and why do) certificates refer to other certificates?
- **Solution** (partial): Extract certificate IDs via regex, canonicalize

# Certificate references

- **Question:** What **(and why do)** certificates refer to other certificates?
- **Solution** (partial): Extract certificate IDs via regex, canonicalize
- The **reasons** are a hard problem
  - Component
  - Re-certification
  - Simultaneous certification
  - ...
- **Future work:** Try Natural Language Processing

# Web frontend



- Browsing
  - CC and FIPS 140 certificates
- Search and filtering
  - Full-text search of certification documents
- Data
  - Daily updates
  - JSON export available
- Notifications
  - Subscribe via email
  - Notified on changes
  - Notified on new vulnerabilities

## DEMO



Certificate



References

# Use-cases

## **Vulnerability researchers**

- Information on certified products

# Use-cases

## **Vulnerability researchers**

- Information on certified products

## **Evaluation labs**

- Where the space is moving



# Use-cases

## **Vulnerability researchers**

- Information on certified products

## **Evaluation labs**

- Where the space is moving

## **Vendors**

- What competitors are doing

# Use-cases

## **Vulnerability researchers**

- Information on certified products

## **Evaluation labs**

- Where the space is moving

## **Vendors**

- What competitors are doing

## **End-users**

- Notification for vulnerabilities







**Thanks!**

 J08nY |  neuromancer.sk |  jan@neuromancer.sk

Icons from  **Font Awesome**

Photos from  **Unsplash**

# Resources

-  <https://unsplash.com/photos/9V5GssdEG-4>
-  <https://unsplash.com/photos/snNHKZ-mGfE>
-  <https://imgflip.com/memegenerator/74331809/Pepe-Silvia>
-  <https://unsplash.com/photos/pAyN5zqdqDo>