

Security of National eID (smartcard-based) Web Applications



Raul Siles
raul@taddong.com
NCSC Conference 2013
January 22-23, 2013



- Introduction to eID
- eID security state-of-the-art
- Pen-testing eID web-apps
 - HTTPS, eID & session management
- Results & Recommendations from real-world pen-tests
 - HTTPS, eID & session management
- Conclusions

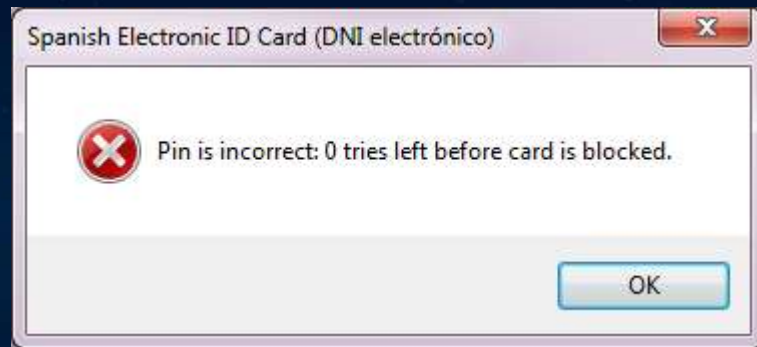
eID (or e-ID)



- (National) electronic IDentification (eID)
 - Username/password, mobile, **smartcard**...
- By example: Spanish eID (DNle or eDNI)
 - DNle internal layout
 - Zones: public, private (PIN) & security
 - Biometric data (fingerprint, picture y signature)
 - ISO 7816 (PKCS#15 evolution)
 - Certificates (& two associated key-pairs)
 - Identification (KeyUsage = Digital Signature)
 - Signature (KeyUsage = contentCommitment)
 - Legal validity & CWA 14169: Secure signature-creation device (EAL4+)



The eID is Secure...



Real eID Security Threats



- Physical eID access and PIN knowledge
- End-user computer compromised
- Examples: (eID/*smartcards*)
 - “Man-In-Remote: PKCS11 for fun and non-profit”. Gabriel González. RootedCON 2011
 - Remote PIN & PKCS#11 invocation
 - Sykipot trojan variant – China (AlientVault)
 - US DoD *smartcards* PIN acquisition
 - Keylogger + Windows certs. memory access
 - Remote user impersonation (*proxy*)
 - December 2011 (March?)

The eID is Secure, But... Where Is It Being Used?



Who Has an eID? (in Spain)

- +32 million eIDs dispatched (December, 2012)
 - Project started in 2005
 - Around 65% of the Spanish population
- Spain is a **worldwide leader in electronic signature-based smartcards** (electronic ID)
 - 26 countries all over the world (smartcard & signature)
- National Home Office (police department)
 - +1,500 dispatch offices (+341M €)

<http://www.mir.es/press/la-policia-nacional-supera-los-25-millones-de-dni-electronicos-expedidos-12920>

What Do We Use the eID For?



- Personal Computers
 - Login (user authentication)
 - Sign documents (e.g. invoices)
 - Get access to Wi-Fi and VPN networks
 - VoIP call authentication...



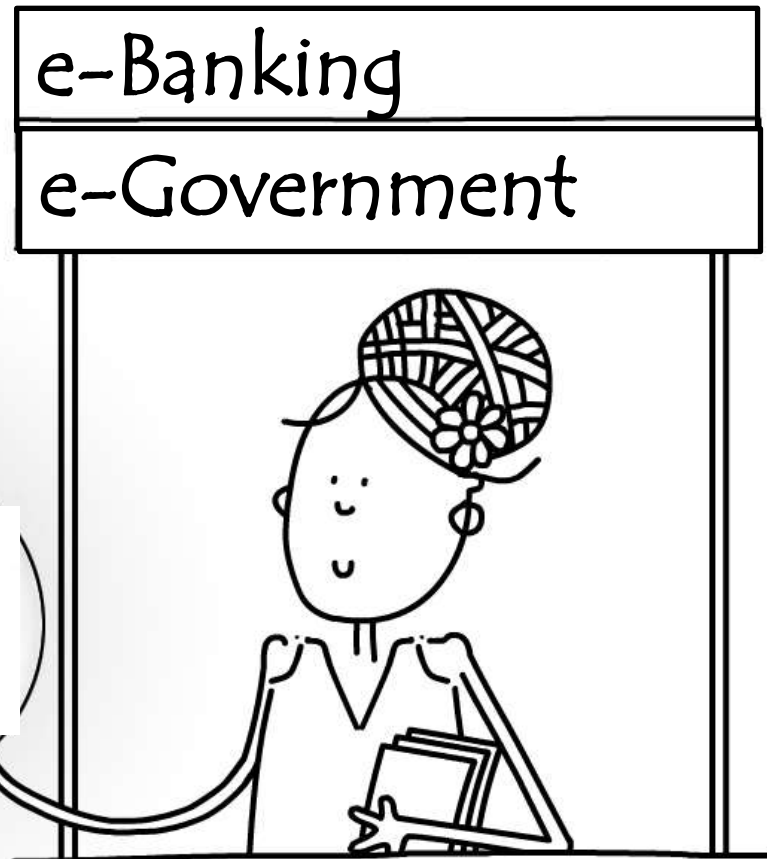
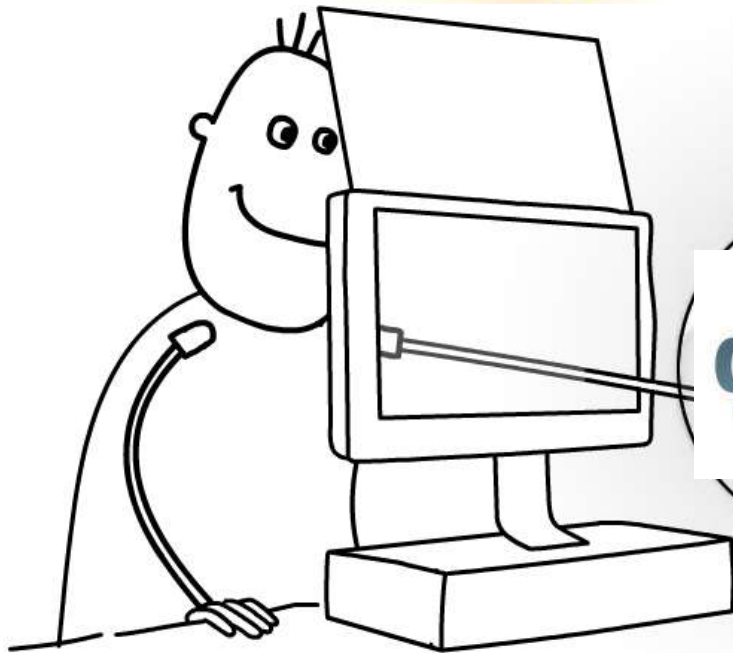
- Madrid & Barcelona airports
 - Automatic frontier control project
 - ABC System (Indra) & National police
 - Self-service
 - eID + picture + fingerprint



- ATMs
- TDT (eAdmin via digital TV)
- Mobile phones (mDNI)



What Do We Use the eID For? In Reality...



eID is Used in Web-Apps



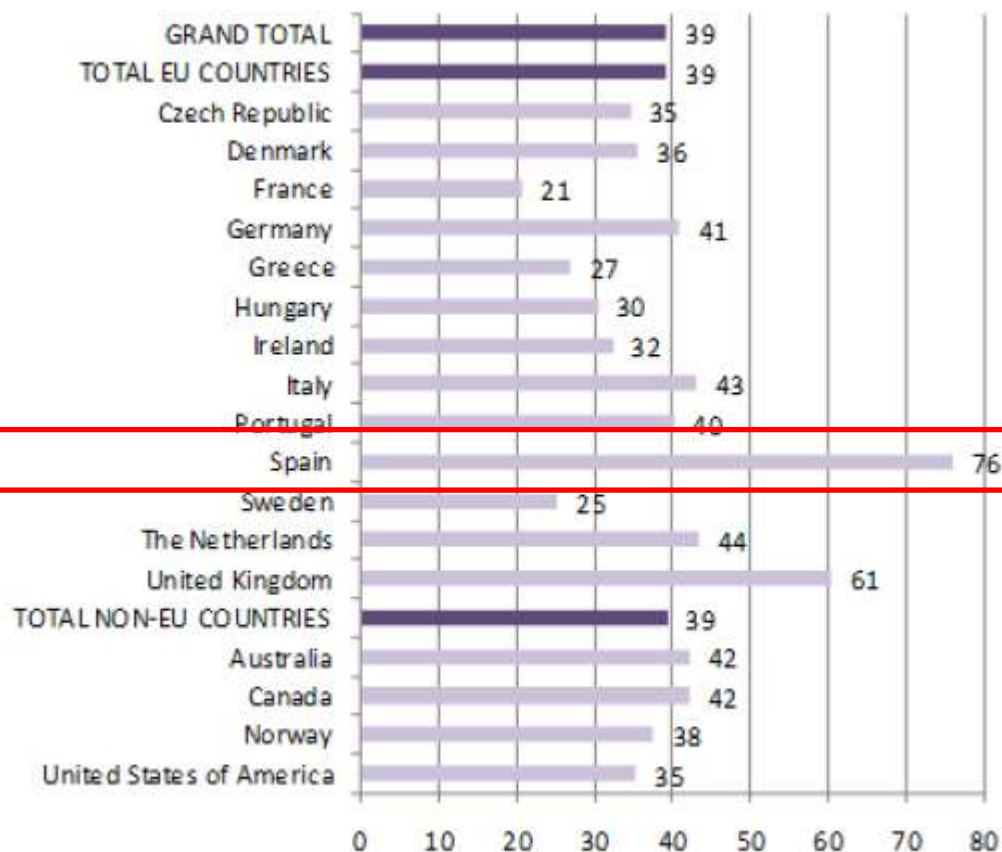
- Critical web applications
 - Public sector
 - e-Government services
 - March 2011: 2,015 online services
 - 99% procedures from the Central Government
 - Private sector
 - Financial (e-Banking), insurance, and utility companies (telecom, electricity, water, gas...)
 - e-Commerce
 - Most secure authentication method
 - Username/password (backup)



eAccessibility vs. eSecurity



Status of Web content accessibility (government websites), by country



Source: Monitoring eAccessibility in Europe: 2011 Annual Report.

Unit: Percentages

European eID Regulation



- European Commission Press Release
 - June 4, 2012 (... 2014)
- Digital Agenda: new Regulation to enable cross-border electronic signatures and to get more value out of electronic identification in Digital Single Market
 - National electronic identification schemes (eIDs)
 - Electronic identification, signatures and trust services
 - Acceptance of cross-country citizen transactions



<http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/558>
<http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/403>

eID by Country



- eID (EU): smartcard
 - Belgium, Estonia, Finland, Germany, Italy, Portugal, Spain, Switzerland
- Pseudo eID (EU): user/pass + SMS, cert...
 - Austria (2), Czech Republic, Denmark, Holland, Iceland, Liechtenstein, Lithuania, Luxemburg, Slovakia, Slovenia, Sweden
 - Holland (July 2012) + 7 years
 - DigID 4.0: username & password (+ SMS code)
 - Future: Smartcard-based eID...
- Outside EU
 - Hong-Kong, Morocco, Saudi Arabia, South Korea, UAE



The eID is Secure, It Is Used in
Web-Apps, World-Wide, But...
Is It Used in a Secure Way?



eID (Smartcard-Based) Web Applications



- eID web-based authentication
 - HTTPS protocol
 - Standard and transparent solution
 - Built-in client-based digital certificate (X.509) authentication in all web browsers
 - Web-based client components
 - Custom Java Applet or ActiveX control
 - eID cloud-based authentication
- eID web-based signatures
 - Web-based client components or JavaScript
 - JS: Proprietary IE (CAPICOM) o Firefox (crypto.signText())
 - Client components: local permissions required?





Pen-Testing eID Web-Apps

Get Authorization



Pen-Testing eID Web-Apps

Research Areas



1



2



3





HTTPS



HTTPS Authentication: Client Certs.

1

DNle_auth_dnie.es_FULL.pcap - Graph Analysis

Time	192.168.1.207	213.170.35.240	Comment
0,049	54510 > https [SYN]		TCP: 54510 > https [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
0,116	https > 54510 [SYN]		TCP: https > 54510 [SYN, ACK] Seq=0 Ack=1 Win=4356 Len=0 MSS=1452 WS=1 SACK_PERM=1
0,116	54510 > https [ACK]		TCP: 54510 > https [ACK] Seq=1 Ack=1 Win=66792 Len=0
0,117	Client Hello		TLsv1: Client Hello
0,184	https > 54510 [ACK]		TCP: https > 54510 [ACK] Seq=1 Ack=185 Win=4540 Len=0
0,186	Server Hello		TLsv1: Server Hello
0,190	TCP segment of a r		TCP: [TCP segment of a reassembled PDU]
0,190	TCP segment of a r		TCP: [TCP segment of a reassembled PDU]
0,190	54510 > https [ACK]		TCP: 54510 > https [ACK] Seq=185 Ack=1524 Win=66792 Len=0
0,191	Certificate		TLsv1: Certificate
0,191	Certificate Request		TLsv1: Certificate Request
0,191	54510 > https [ACK]		TCP: 54510 > https [ACK] Seq=185 Ack=2222 Win=66092 Len=0
0,192	Server Hello Done		TLsv1: Server Hello Done
0,203	TCP segment of a r		TCP: [TCP segment of a reassembled PDU]
0,289	https > 54510 [ACK]		TCP: https > 54510 [ACK] Seq=2231 Ack=1637 Win=5992 Len=0
0,289	Certificate, Client		TLsv1: Certificate, Client Key Exchange
0,357	https > 54510 [ACK]		TCP: https > 54510 [ACK] Seq=2231 Ack=3322 Win=7677 Len=0
1,985	Certificate Verify		TLsv1: Certificate Verify
1,985	Change Cipher Spec		TLsv1: Change Cipher Spec
1,985	Encrypted Handshake		TLsv1: Encrypted Handshake Message
2,052	https > 54510 [ACK]		TCP: https > 54510 [ACK] Seq=2231 Ack=3589 Win=7944 Len=0
2,053	https > 54510 [ACK]		TCP: https > 54510 [ACK] Seq=2231 Ack=3595 Win=7950 Len=0
2,054	https > 54510 [ACK]		TCP: https > 54510 [ACK] Seq=2231 Ack=3632 Win=7987 Len=0
2,056	Change Cipher Spec		TLsv1: Change Cipher Spec
2,056	Encrypted Handshake		TLsv1: Encrypted Handshake Message
2,056	54510 > https [ACK]		TCP: 54510 > https [ACK] Seq=3632 Ack=2274 Win=66040 Len=0
2,057	Application Data		TLsv1: Application Data

Save As Close

Assessing HTTPS (SSL/TLS)

1

- TLSSLed (v1.2 - October 2011)
 - Web server SSL/TLS (HTTPS) implementation security assessments
 - sslscan & openssl (GNU/Linux & Mac OS X)
 - SSLv2, SSLv3/TLSv1, TLSv1.1/v1.2 (BEAST), NULL cipher, weak (40/56 bits) & strong (AES 128/256 bits) ciphers, MD5-signed certs., cert. key length, subject, issuer (CA), validity period, STS header, (un)secure cookies, RFC 5746: secure SSL/TLS renegotiation...
 - *Upcoming v1.3 adds new features...*

<http://blog.taddong.com/2011/10/tlssled-v12.html>





eID



Assessing eID Integration in Web-Apps

2

- In-depth web-app security analysis
 - Registration & authentication using the eID
 - Access controls
- Interception proxies: smartcard constraints
 - Commercial & open-source tools (Java)
 - Client certificate errors (HTTPS)
 - Need smartcard drivers or libraries
 - Built-in integration required



Main focus: OWASP ZAP...



Session Management



- Top web vulnerabilities: SQLi, XSS, CSRF...
 - Session management? OWASP Top 10 (A3)
- Malware: OddJob (February 2011)
 - Hijacks users sessions and keeps them active
 - US & EU banks



<http://blog.taddong.com/2012/02/owasp-session-management-cheat-sheet.html>
https://www.owasp.org/index.php/Session_Management_Cheat_Sheet



eID: PKCS#11 & Java



PKCS#11 (eID) & Java: Windows



- Statically (e.g. keytool)
 - Based on the OS: Win, Linux or Mac
 - %JAVA_HOME%/lib/security/java.security

```
security.provider.10=sun.security.pkcs11.SunPKCS11 C:/Program Files (x86)/Java/jre6/lib/security/dnie pkcs11.cfg
```

- Configuration file for SunPKCS11:

```
# Provider.getName() = SunPKCS11-DNIE  
name = DNIE  
# DNIE library  
library = C:\WINDOWS\SysWOW64\Usrcpkcs11.dll
```

Install eID libraries 1st...

PKCS#11 (eID) & Java: Linux



- Statically (e.g. keytool)
 - Based on the OS: Win, Linux or Mac
 - `$JAVA_HOME/lib/security/java.security`

```
security.provider.10=sun.security.pkcs11.SunPKCS11  
/usr/lib/jvm/java-6-sun/jre/lib/security/dnie_pkcs11.cfg
```

- Configuration file for SunPKCS11:

```
# Provider.getName() = SunPKCS11-DNIE  
name = DNIE  
# DNIE library  
library = /usr/lib/opensc-pkcs11.so
```

PKCS#11 (eID) & Java: Mac



- Statically (e.g. keytool)
 - Based on the OS: Win, Linux or Mac
 - `$JAVA_HOME/lib/security/java.security`

```
security.provider.10=sun.security.pkcs11.SunPKCS11  
/.../1.6.0.jdk/Contents/Home/lib/security/dnief pkcs11.cfg
```

- Configuration file for SunPKCS11:

```
# Provider.getName() = SunPKCS11-DNIE  
name = DNIE  
# DNIE library  
library = /usr/lib/opensc-pkcs11.so
```

32-bit Java VM:
\$ java -d32 ...

PKCS#11 (eID) & Java: Query eID



- Java keytool (e.g. Windows)
 - List eID contents (PKCS11 token)

```
C:\> keytool [-v] -keystore NONE -storetype PKCS11 -list
Escriba la contraseña del almacén de claves: ...
```

- With no provider setup in java.security

```
C:\> keytool -keystore NONE -storetype PKCS11
      -providerClass sun.security.pkcs11.SunPKCS11
      -providerArg "C:\Program Files (x86)\Java\jre6\
                   \lib\security\dnies pkcs11.cfg"
      -list
```

PKCS#11 (eID) & Java: Code



```
...  
// Add PKCS11 provider  
String cardConfig = "dnie_pkcs11.cfg"; // or InputStream  
Provider pkcs11 = new sun.security.pkcs11.SunPKCS11(cardConfig);  
Security.addProvider(pkcs11);  
  
// Init the keystore  
KeyStore ks = KeyStore.getInstance("PKCS11", pkcs11);  
ks.load(null, pin.toCharArray());  
  
KeyManagerFactory kmf = KeyManagerFactory.getInstance("SunX509");  
kmf.init(ks, pin.toCharArray());  
KeyManager[] kms = kmf.getKeyManagers();  
  
X509TrustManager trustManager = new X509TrustManager() { ... }  
TrustManager[] tms = new TrustManager[] {trustManager};  
  
// Init SSL context  
SSLContext sc = SSLContext.getInstance("SSL");  
sc.init(kms, tms, new java.security.SecureRandom()); ...
```

OWASP ZAP: Zed Attack Proxy



- Web interception proxy & much more...
 - Open source (Java)
 - Multiplatform: Windows, Linux & Mac OS X
 - Paros & Andiparos (& WebScarab) evolution
- Supports client-based certs. & smartcards
 - Tools - Options - Certificate
 - Keystore: PKCS11, PKCS12...
 - Unsecure SSL/TLS renegotiation
 - eID failed access attempts (PIN): PUK



https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
<http://code.google.com/p/zaproxy/>

ZAP DNle Support



- PKCS#11 (after installing the DNle drivers...)
 - ① – Windows: (XP & 7 – 32 & 64 bits)
 - C:\Windows\System32\UsrPkcs11.dll
 - C:\Windows\SysWOW64\UsrPkcs11.dll
 - ② – GNU/Linux: /usr/lib/opensc-pkcs11.so (or /usr/lib64/)
 - ③ – Mac OS X: /Library/OpenSC/lib/opensc-pkcs11.so
 - /usr/lib/opensc-pkcs11.so (link) & Java 32 bits
- drivers.xml (**OWASP ZAP SmartCard Project**)

<http://blog.taddong.com/2012/04/owasp-zap-smartcard-project.html>

How To Get The Slot (eID & OS)?



- Adding support for new eIDs (or countries)
 - keytool -D... (debug)

```
C:\> keytool -keystore NONE -storetype PKCS11 -list  
-J-Djava.security.debug=sunpkcs11,pkcs11  
Escriba la contraseña del almacén de claves: ...
```



– Result:

Install eID libraries 1st...

```
...  
All slots: 1 (ó 0,1,2,3..., 15)  
Slots with tokens: 1  
Slot info for slot 1:  
...  
Token info for token in slot 1:  
label: DNI electrónico ...
```

The eID is Secure, It Is Used in
Web-Apps, Now We Can Assess Its
Security, So... (Again) Is It Used in a
Secure Way?



Results & Recommendations
From Real-World Pen-Tests

Motivation, Scope & Goals



- Multiple penetration tests on eID-based web applications
 - Both national public and private sectors
 - Different online services (web-apps) using the eID for user authentication (Java, ASP .NET, PHP...)
 - May-December, 2011
- Security assessments focused on authentication (eID), access controls, and session management
 - Beyond SQLi, XSS, XSRF...
- Target web-apps: 15 (very relevant ones)

Pen-Testing eID Web-Apps

Vulnerable Areas



1



2



3



Impact of Vulnerable Areas



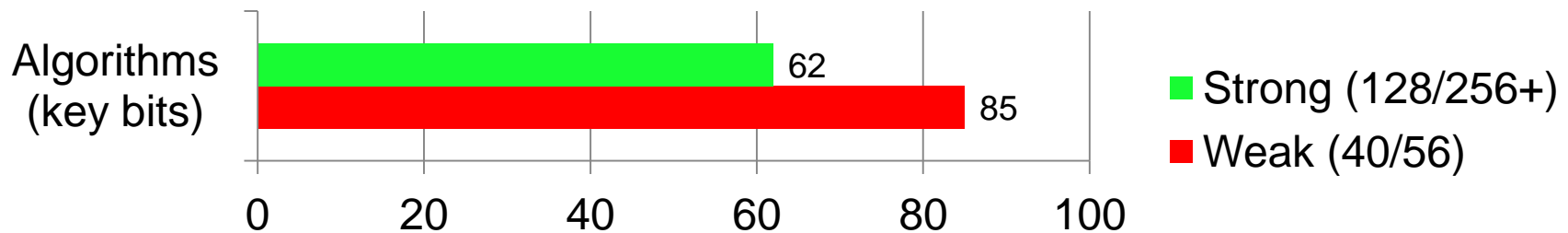
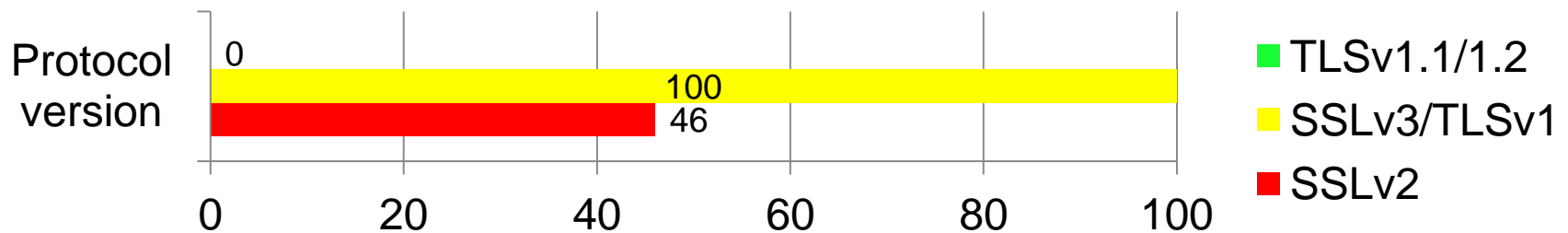
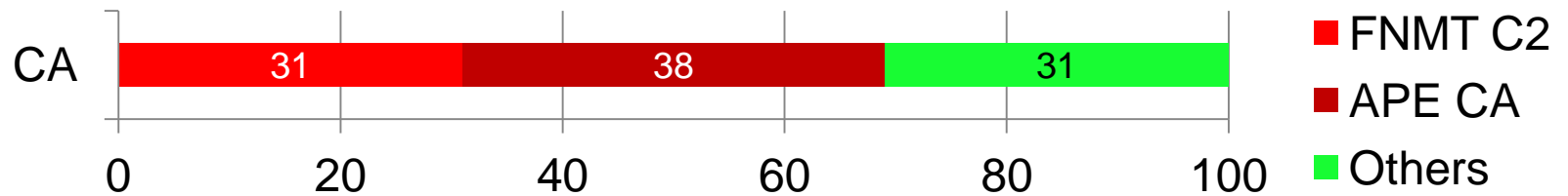
- 1 HTTPS (SSL/TLS) implementation
 - Native integration with eID & client digital certificates
 - Web traffic decryption, MitM attacks, DoS, etc
- 2 eID-based user authentication and registration
 - Manipulate authentication & registration data
 - Complete user impersonation (citizens)
- 3 Web-app session management
 - eID = session ID (cookie)
 - Complete user impersonation (citizens)

...but the eID is secure (we are were confident)

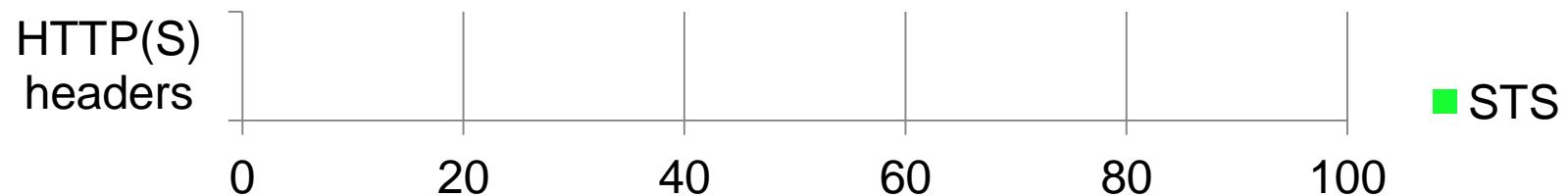
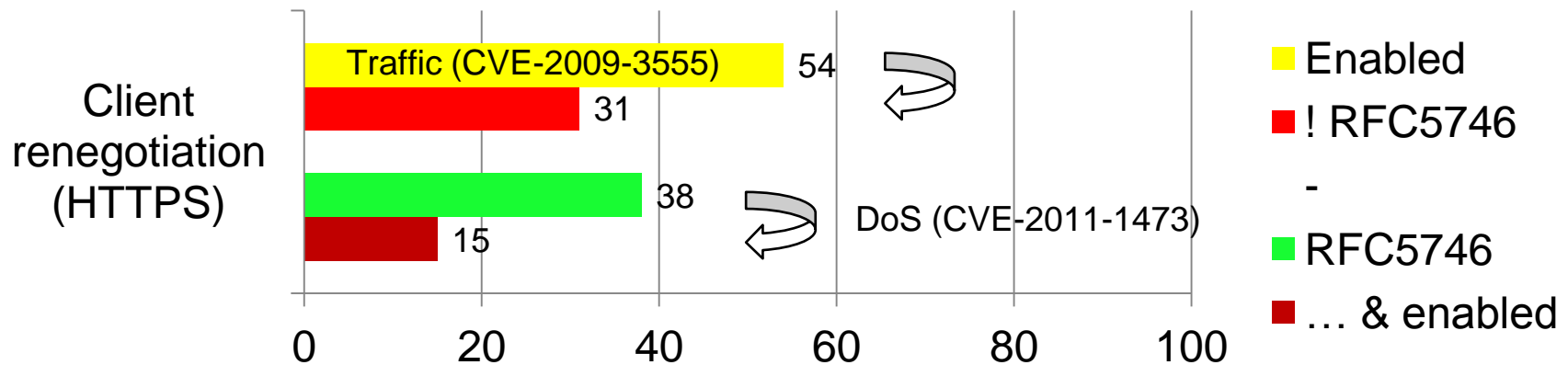
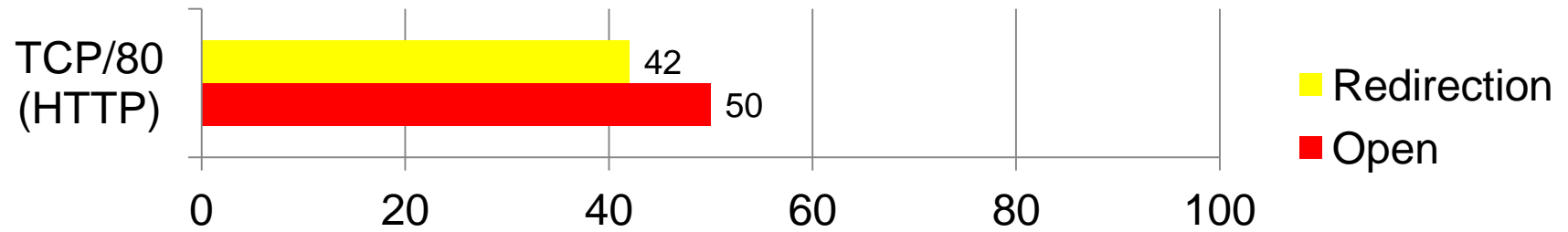
HTTPS



HTTPS Results (1/2)



HTTPS Results (2/2)



HTTPS Renegotiation



- Secure HTTPS (SSL/TLS) renegotiation



eID

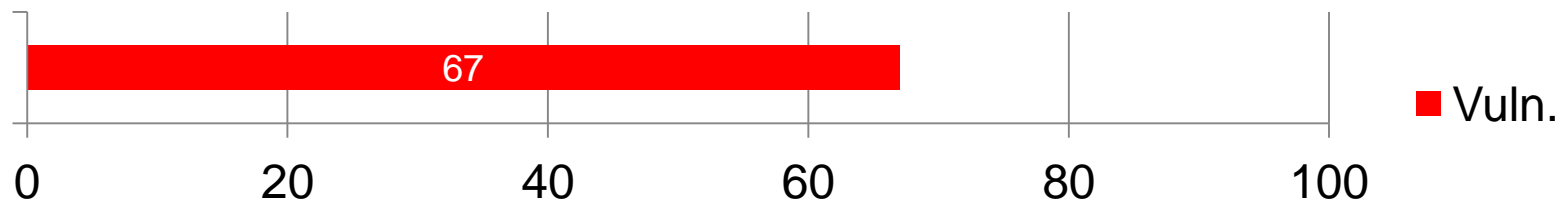
(User Authentication and Registration)



eID-based User Registration Results



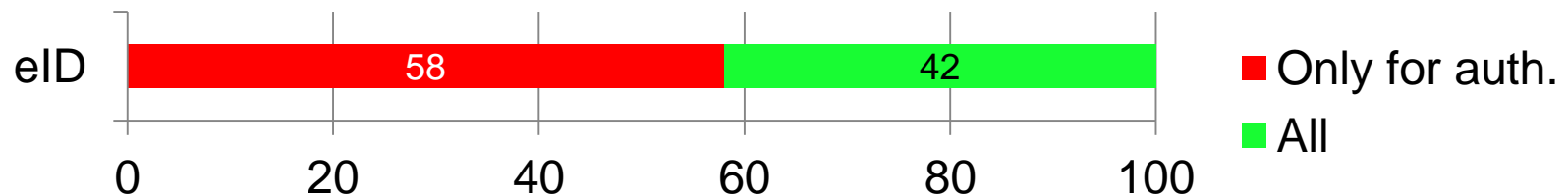
- Web-app requires user registration (eID)
 - Step 1: eID authentication
 - Step 2: Registration details web form
 - Lack of verification?
 - It is possible to manipulate all the victim user info: ID, name & surname, address, phone...
- Is it possible to manipulate registration details?
 - Only 25% web-apps required registration



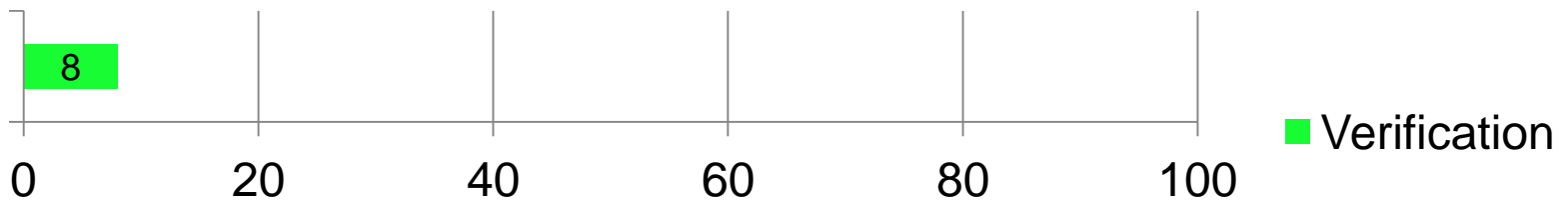
eID-based Authentication Results



- One or multi-step procedures and proceedings
- Is the eID required to access all resources?
 - User impersonation: anonymously or eID



- Matching between eID and session ID



Session Management



Session ID = Credentials



- Session management attacks trying to bypass advanced authentication mechanisms
- ID is equivalent (temporarily) to...
 - PIN & Passwords
 - Passphrases
 - Certificates
 - Smartcards
 - Biometry



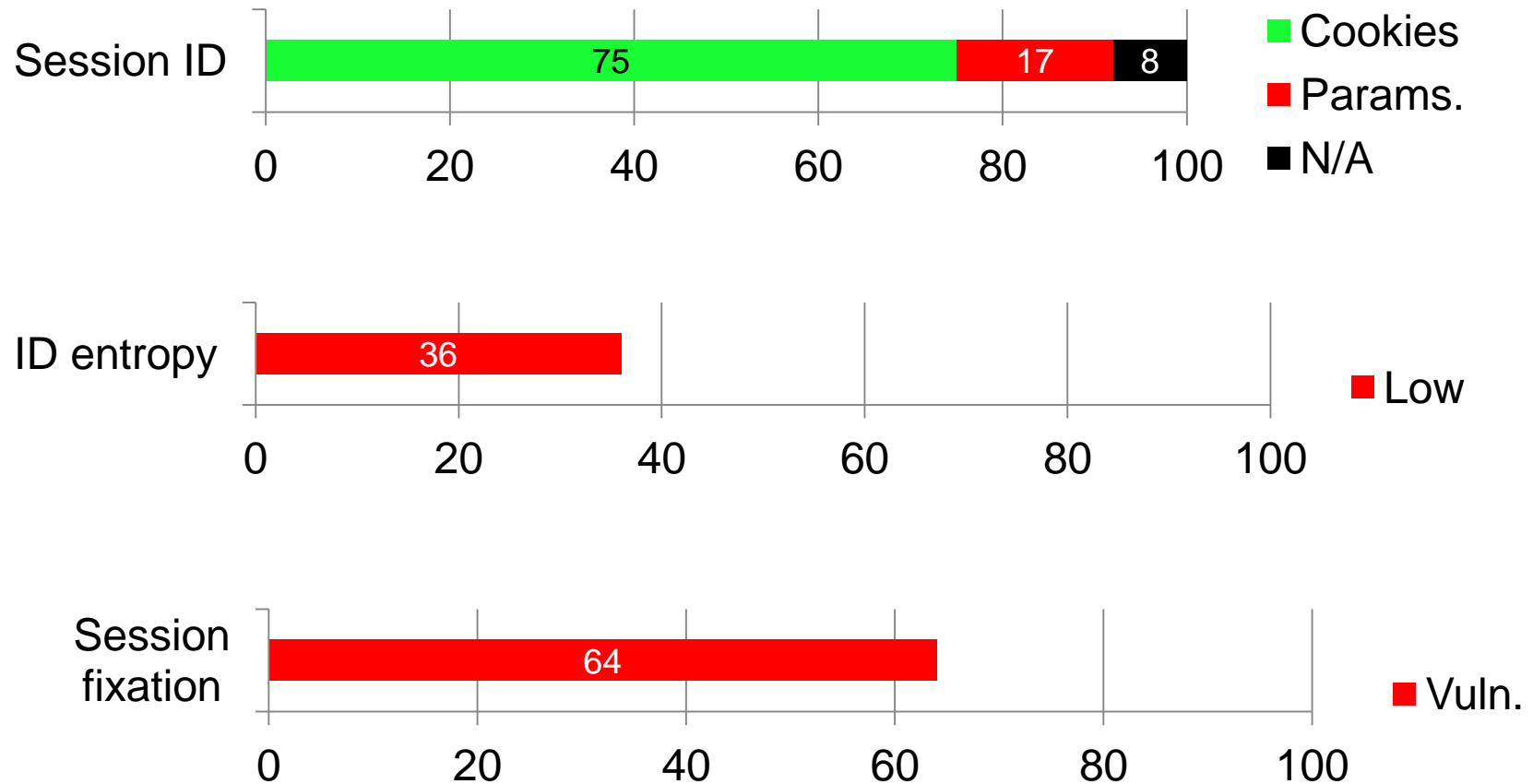
So The eID in Reality is Like...



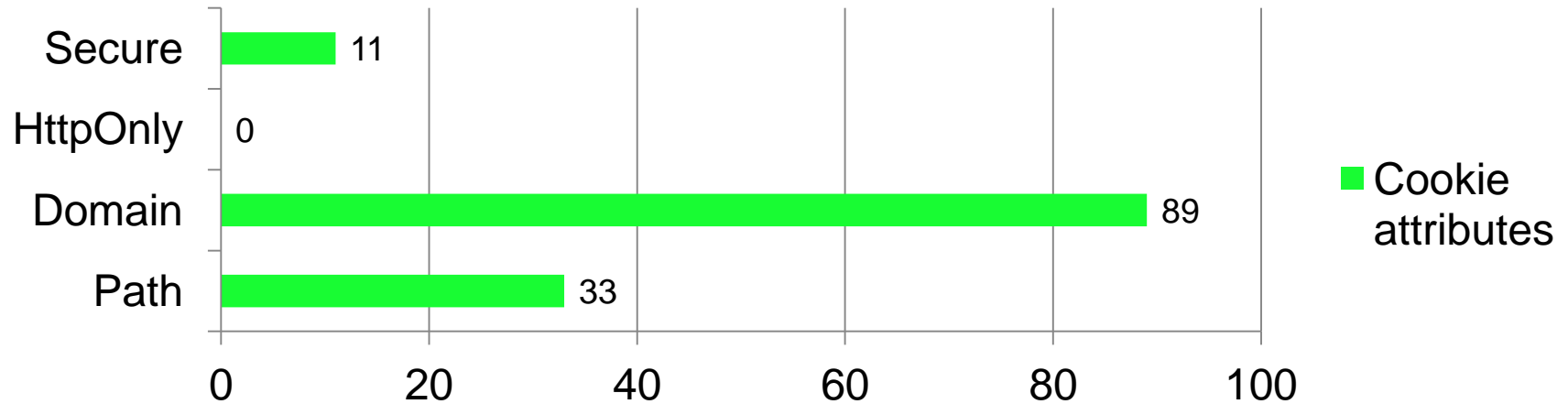
=



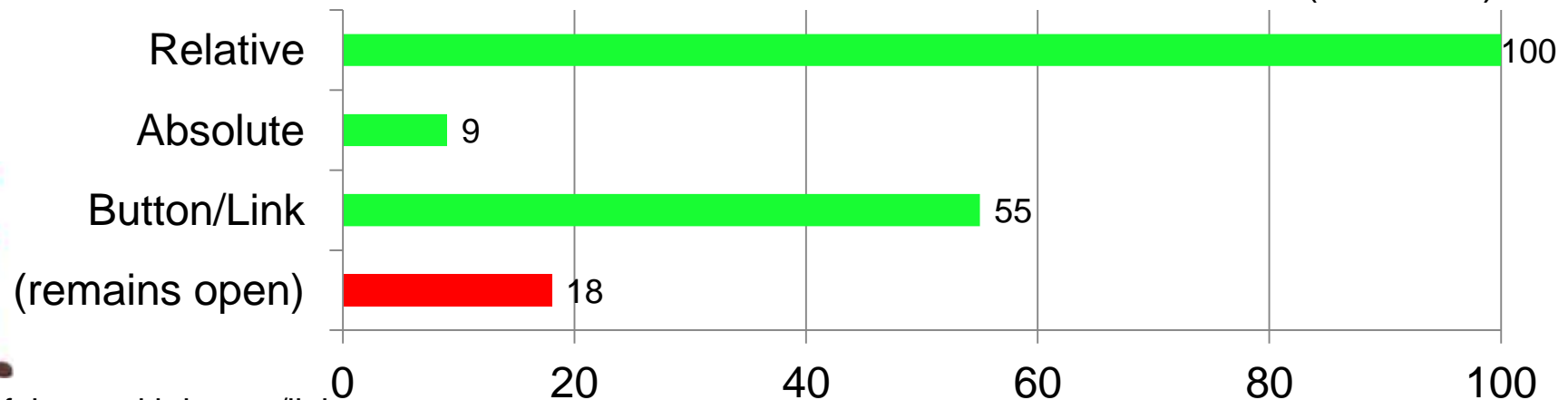
Session Management Results (1/2)



Session Management Results (2/2)



Session finalization (timeouts):



33% of those with button/link

The eID is Secure, It Is Used in
Web-Apps, But... It Seems It Is NOT
Being Used in a Secure Way



Conclusions

Conclusion



Warning



www.sarda.es



Solution



Thank You



Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie





Taddong

www.taddong.com

@taddong