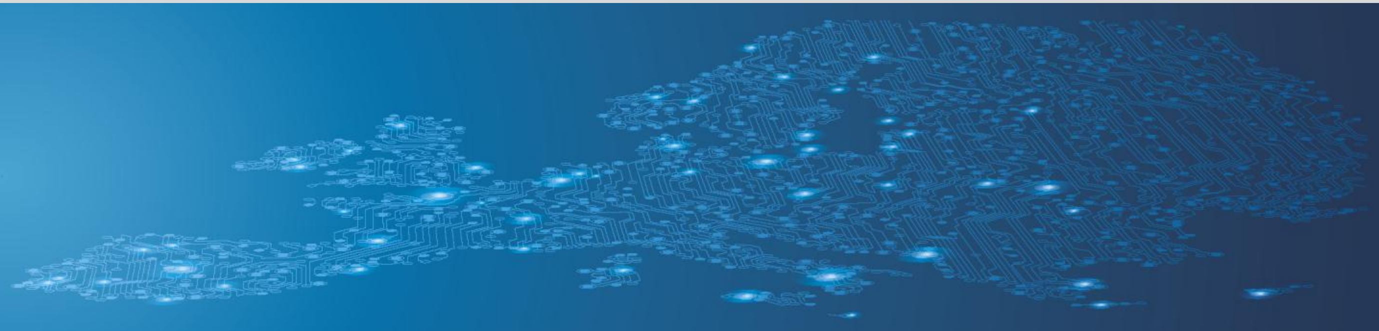
Security Aspects of Trust Services Providers

European Union Agency for Network and Information Security

24th September 2013



Today’s agenda

- 09:30-10:00 Setting up the scene
- 10:00-10:45 The legal, standartization and certification frameworks of trust service security
- 11:00-12:00 Main security risks for trust service providers
- 12:00-13:00 Security aspects of the new trust services defined in the draft Regulation
- 14:00-15:00 Mitigating the impact of security incidents in trust services providers
- 15:15-16:30 Open discussion among all participants
- 16:30-16:45 Closing remarks

SETTING UP THE SCENE

European Union Agency
for Network and Information Security

- Established in 2004
- Centre of expertise: Writing reports that analyse data on security practices in Europe and on emerging risks (e.g. cloud computing, exercises, national contingency plans)
- Supporting the European Commission & Member States in their policy initiatives (e.g. setting up and training CERTs, seminars for national exercises)
- Facilitating cross-border cooperation (e.g. supporting cyber security exercises)
- Ensuring a coherent pan-European approach (e.g. supporting the implementation of article 13a)

ENISA efforts

- Identification of risks associated with new technologies affecting the daily life of citizens
- Cyber crisis cooperation at EU and international level and development of capabilities
- Facilitating Public-Private cooperation
- Improving transparency of security incidents
- Enabling communities to improve NIS: capacity building with regard to the CERT community and application of good practice for CERTs
- Ensuring a strong EU response to cybercrime
- Supporting R&D investments and strengthen the competitiveness of EU's security industry
- Promote personal data protection

Some history

E-Signatures Directive 1999/93/EC

Revision of the Directive: Regulation on electronic identification and trust services for electronic transactions in the internal market

- First major step in enabling **e-Government services**, which have a big potential to make public services effective and save time and money for businesses as well as for citizens.
- It introduced the electronic signature as a meaningful **equivalent** of the hand-written signatures.

- E-Signatures Directive was successful in facilitating e-Government on the national level, but there are still **significant obstacles for cross-border e-Government services.**
- The EC has launched a complex review of the Directive and in June 2012 introduced a **Draft regulation on electronic identification and trust services.**
- The draft regulation will introduce **mutual recognition** of electronic identification and trust services (electronic signatures, electronic seals, time stamping, certified electronic delivery or website authentication)
- **Article 15** of the draft regulation addresses security requirements including **notification of breaches**.

Example of a breach under Art. 15

Diginotar (Certificate Authority in the Netherlands) incident

Over the summer 2011, a certificate authority in the Netherlands experienced a security breach, allowing attackers to generate fake PKI certificates. The fake certificates, the result of the breach, were used to wiretap the online communications of around half a million citizens. Following the breach many e-Government websites were offline or declared unsafe to visit.

Notification articles in EU legislation

Framework Directive, E-Privacy Directive, e-ID Regulation, Data Protection Regulation

Relevant notification articles

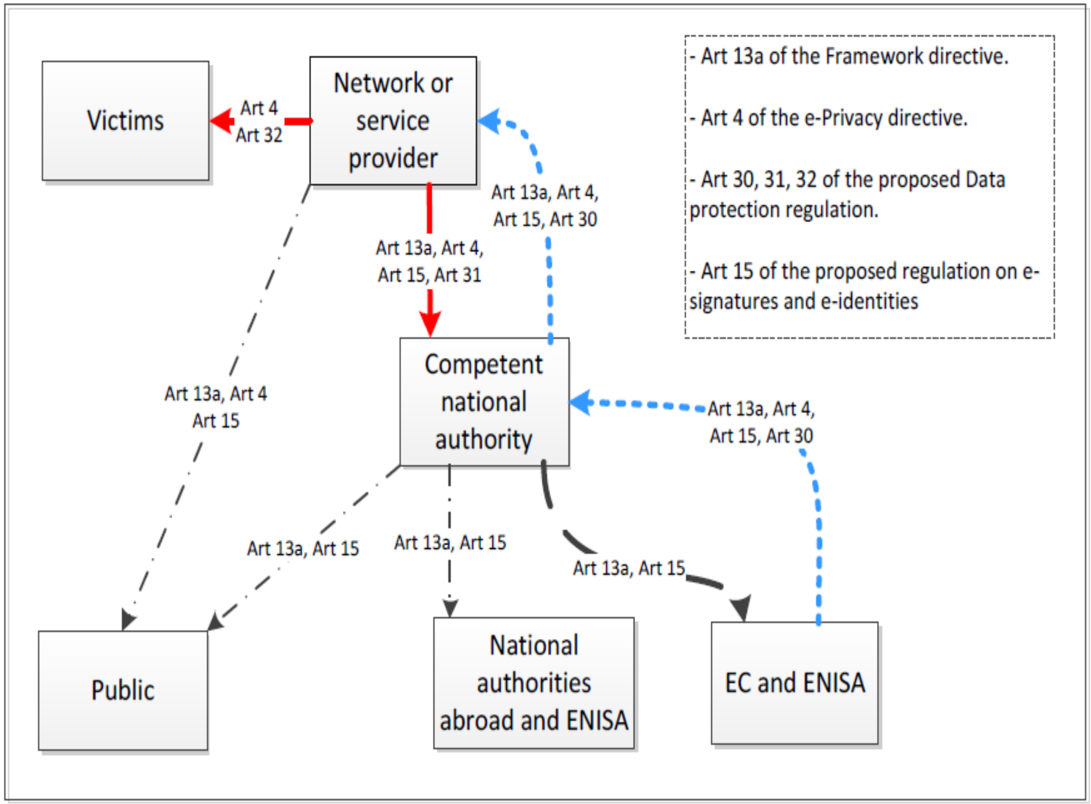
Article 13a of the Framework Directive for electronic communication

Article 4 of the e-Privacy Directive

Article 15 of the Draft Regulation on e-identities

Articles 30, 31 and 32 of the Draft General Data Protection Regulation

Commonalities and diifferences between notification articles


Victims
Network or service provider
Art 4
Art 32
Art 13a, Art 4, Art 15, Art 30
Art 13a, Art 4, Art 15, Art 31
Competent national authority
Art 13a, Art 4 Art 15
Art 13a, Art 4, Art 15, Art 30
Art 13a, Art 15
Art 13a, Art 15
Art 13a, Art 15
Public
National authorities abroad and ENISA
EC and ENISA
- Art 13a of the Framework directive.
- Art 4 of the e-Privacy directive.
- Art 30, 31, 32 of the proposed Data protection regulation.
- Art 15 of the proposed regulation on e-signatures and e-identities

Source: EU Cyber Incident Reporting, ENISA 2012

ENISA Work Programme 2013

- **WPK 1.2**
  - D1: A description of the most important risks identified by the assessment of the processed data, especially when they affect trust infrastructure (technology and services)

  Security aspects of the new trust services defined in the draft Regulation
- **WPK 3.3**
  - D3: good practices for security of electronic identification systems

  Security requirements for Trust Service Providers
  - D4: eID workshop

Security requirements for trust service providers

- **The legal, standartization and certification frameworks of trust service security**
- **Main security risks for trust service providers**
- **Mitigating the impact of security incidents in trust services providers**

This workshop

- **Introduction to initial findings**
- **Hearing of experts opinion**
- **Discussion of issues**
- **Goals**
  - Common understanding
  - Harmonized procedures
  - Verification of guidelines

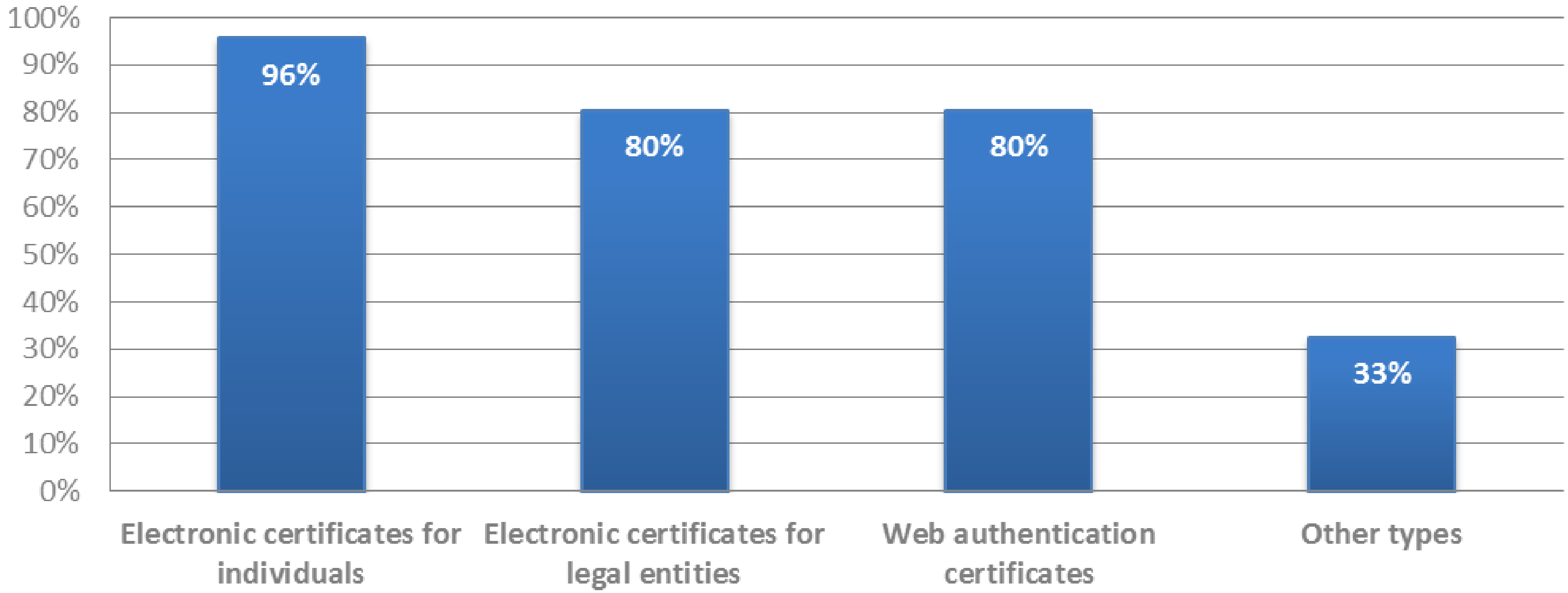
Open questions

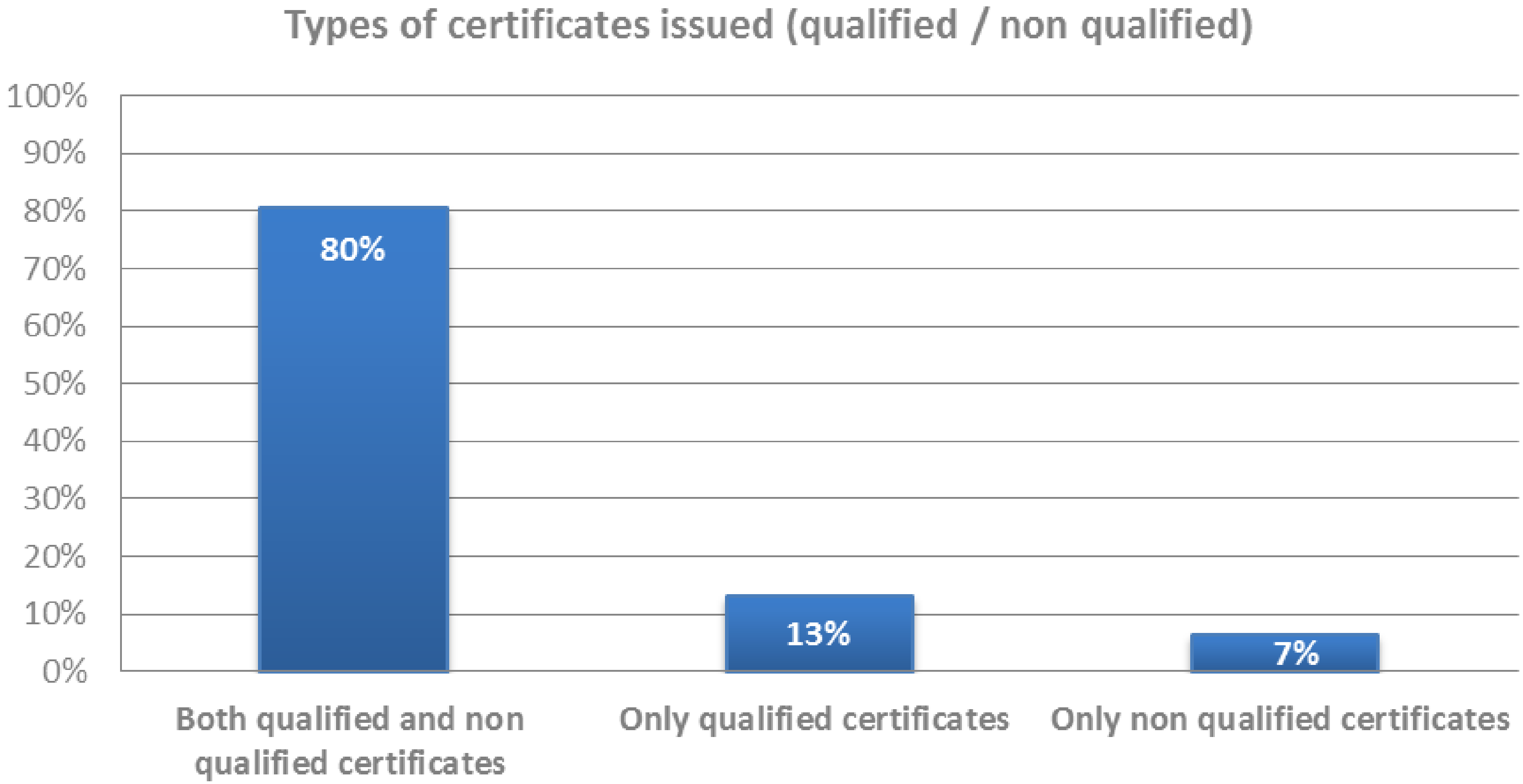
- What the Trust Service Providers expect from the policy makers?
- Are the current approaches effective?
- What could be improved?
- Are the recommendations feasible?

UPDATE ON EIDAS

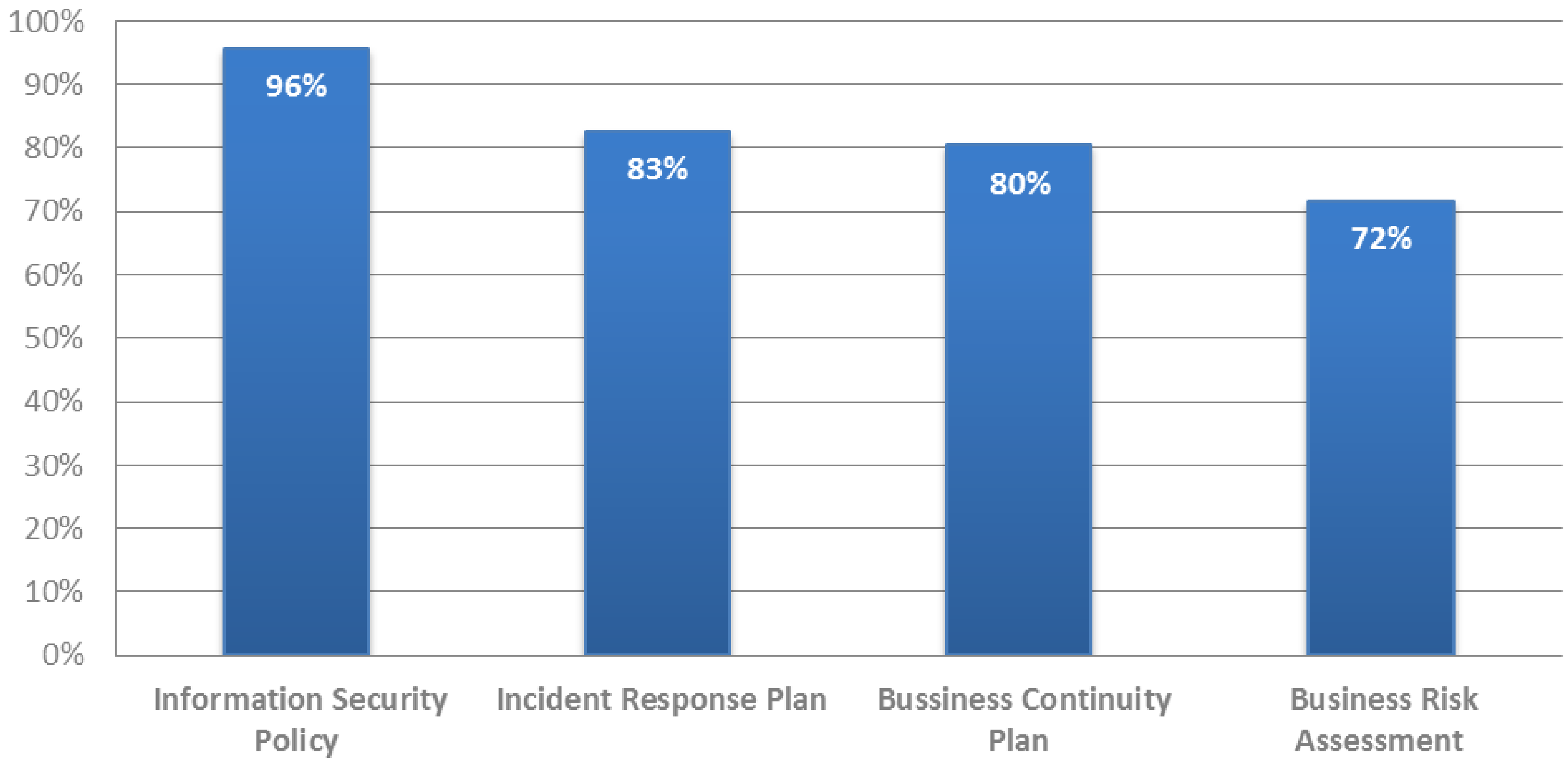
THE LEGAL, STANDARTIZATION AND CERTIFICATION FRAMEWORKS OF TRUST SERVICE SECURITY

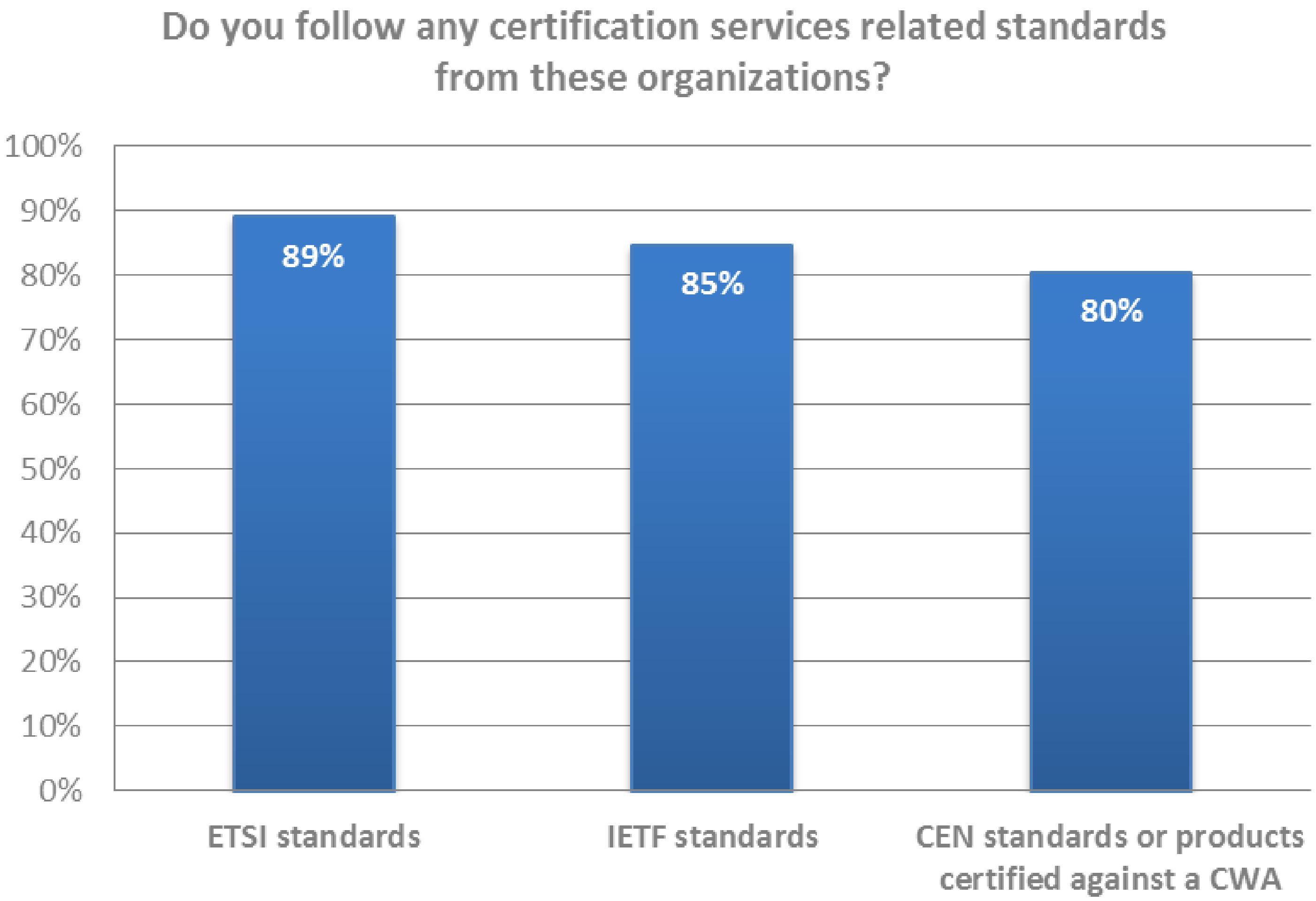
What type of electronic certificates do you provide?



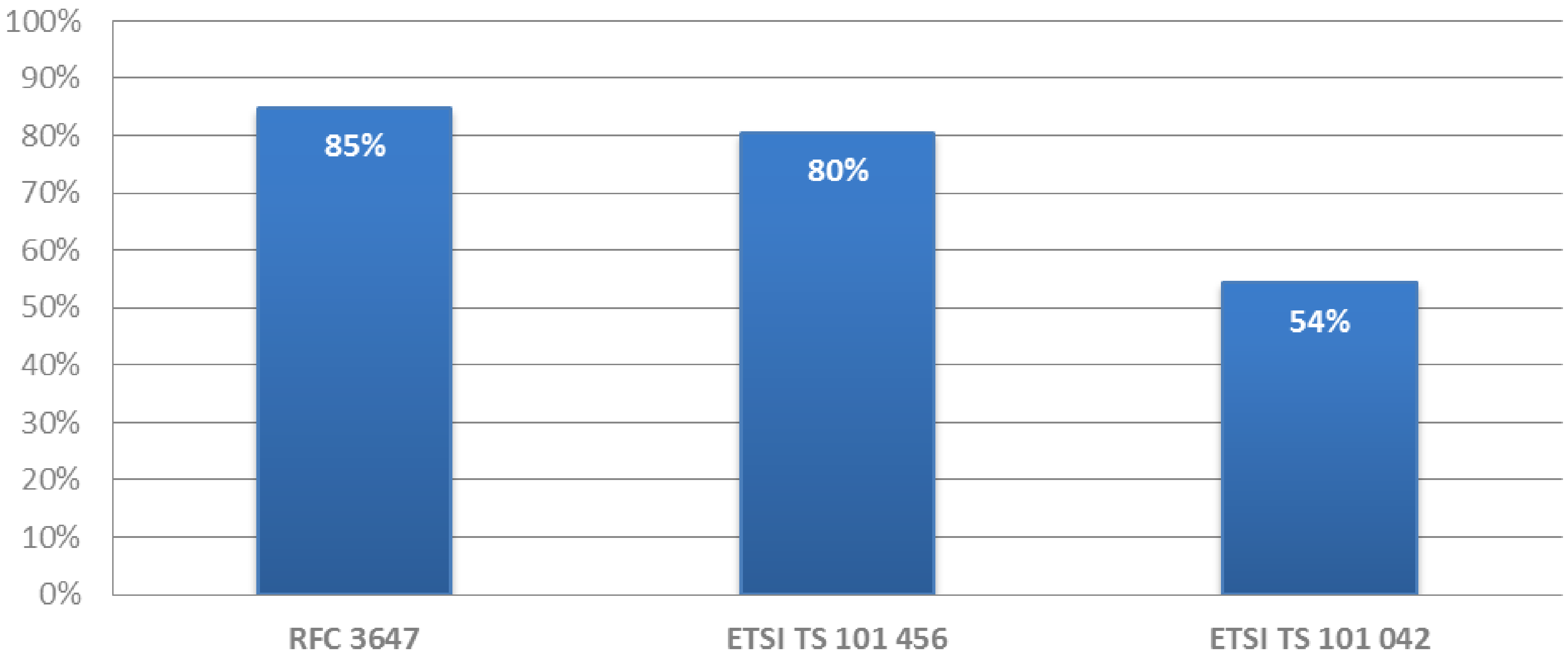

Types of certificates issued (qualified / non qualified)
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
80%
13%
7%
Both qualified and non qualified certificates
Only qualified certificates
Only non qualified certificates

Does your organization have an aproved document for:

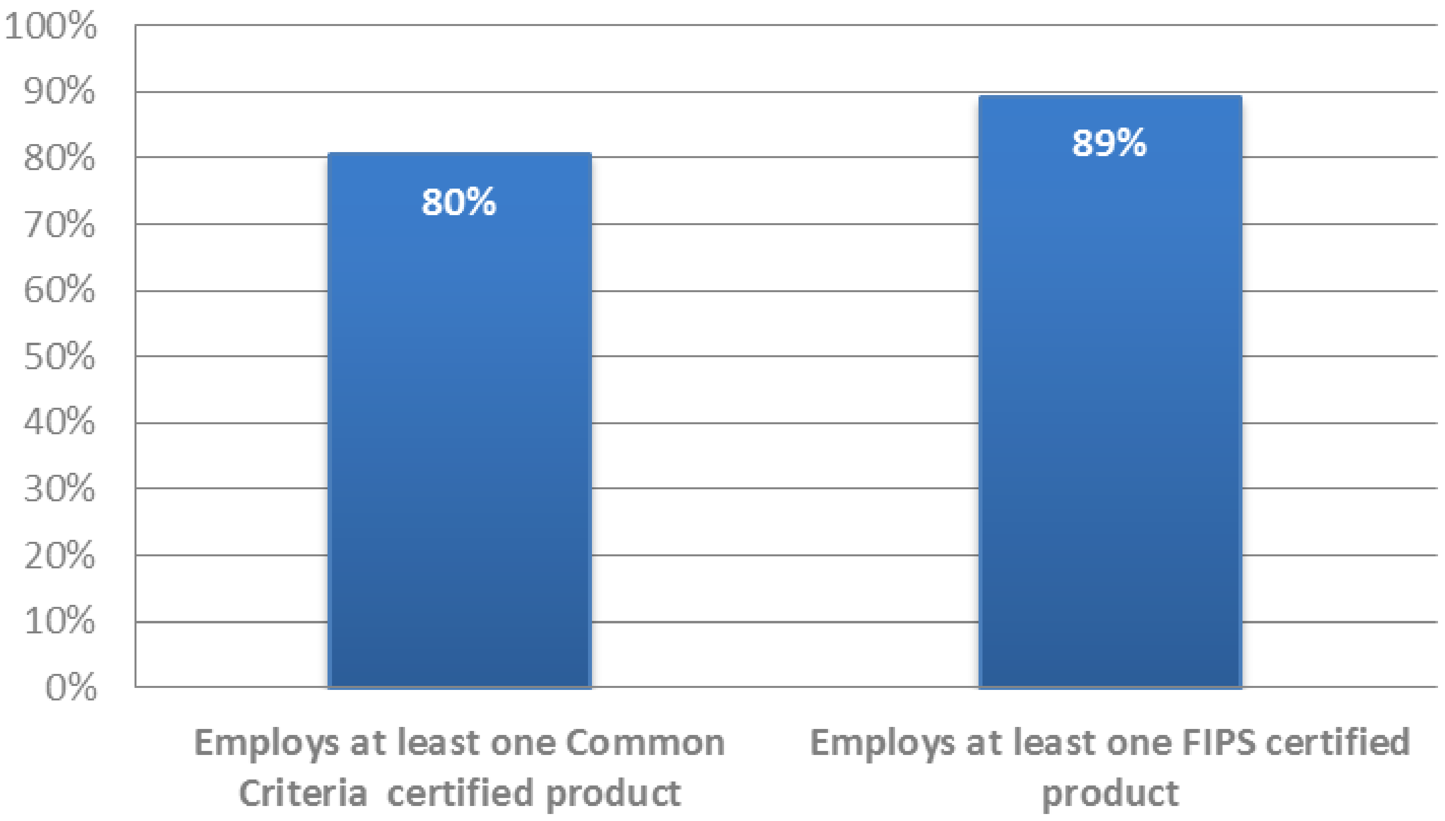



Do you follow any certification services related standards from these organizations?
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
89%
85%
80%
ETSI standards
IETF standards
CEN standards or products certified against a CWA

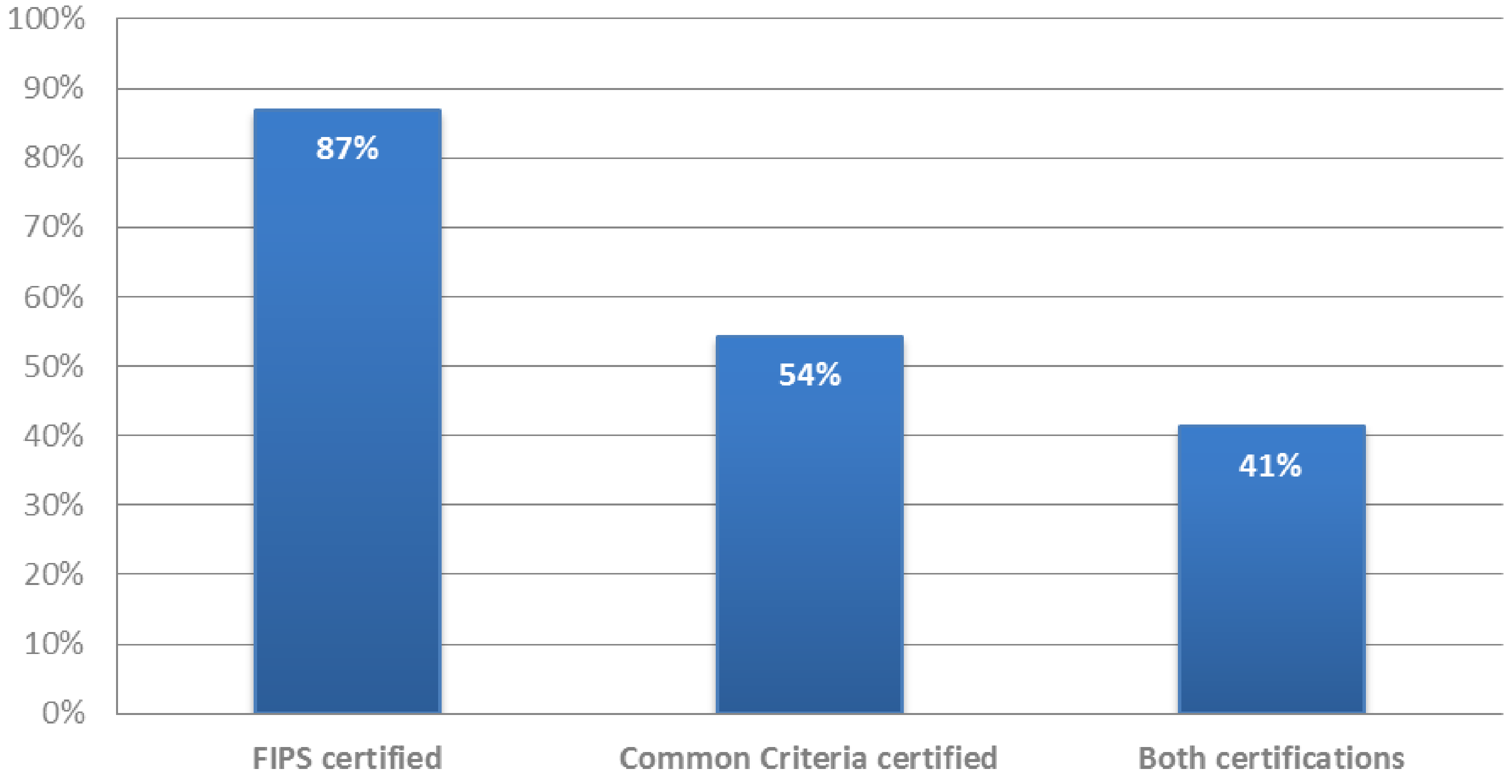
Which standards do you follow for the certification policies and practices?



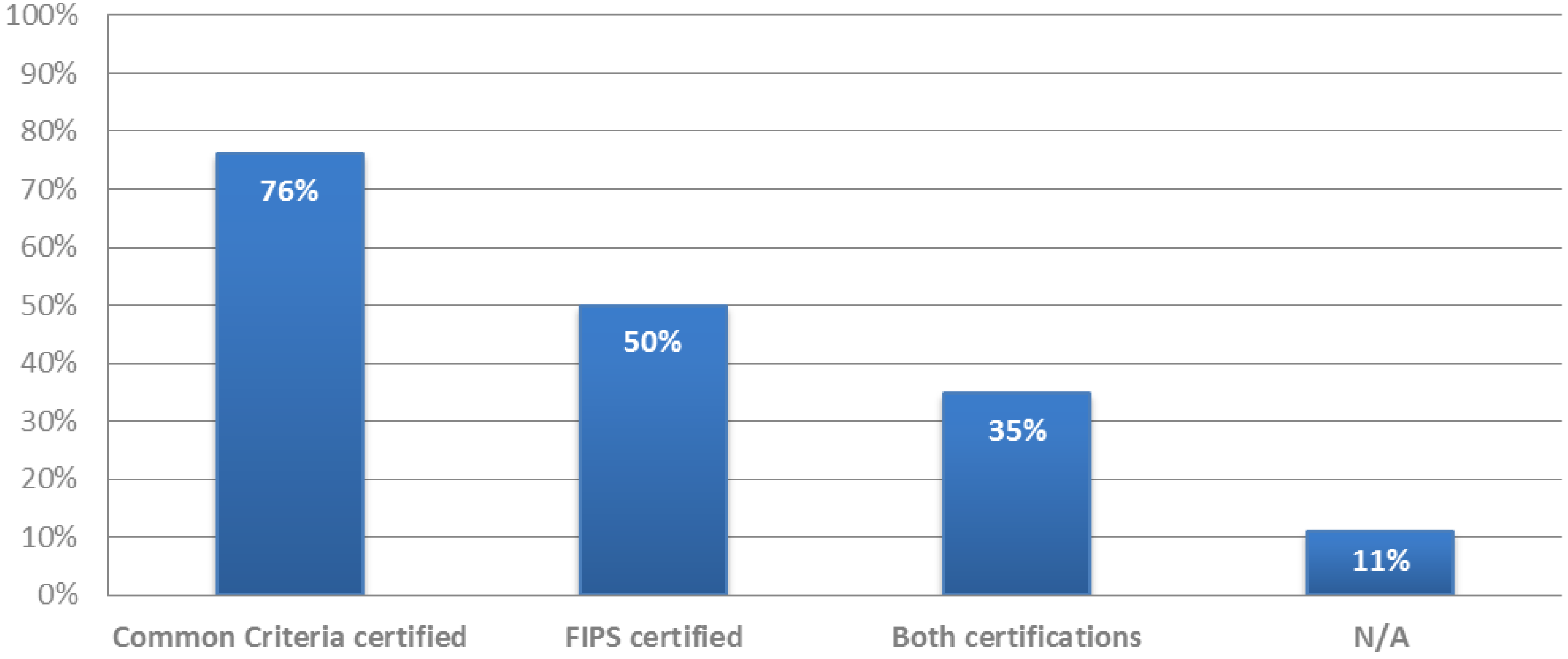
Use of certified signature generation products



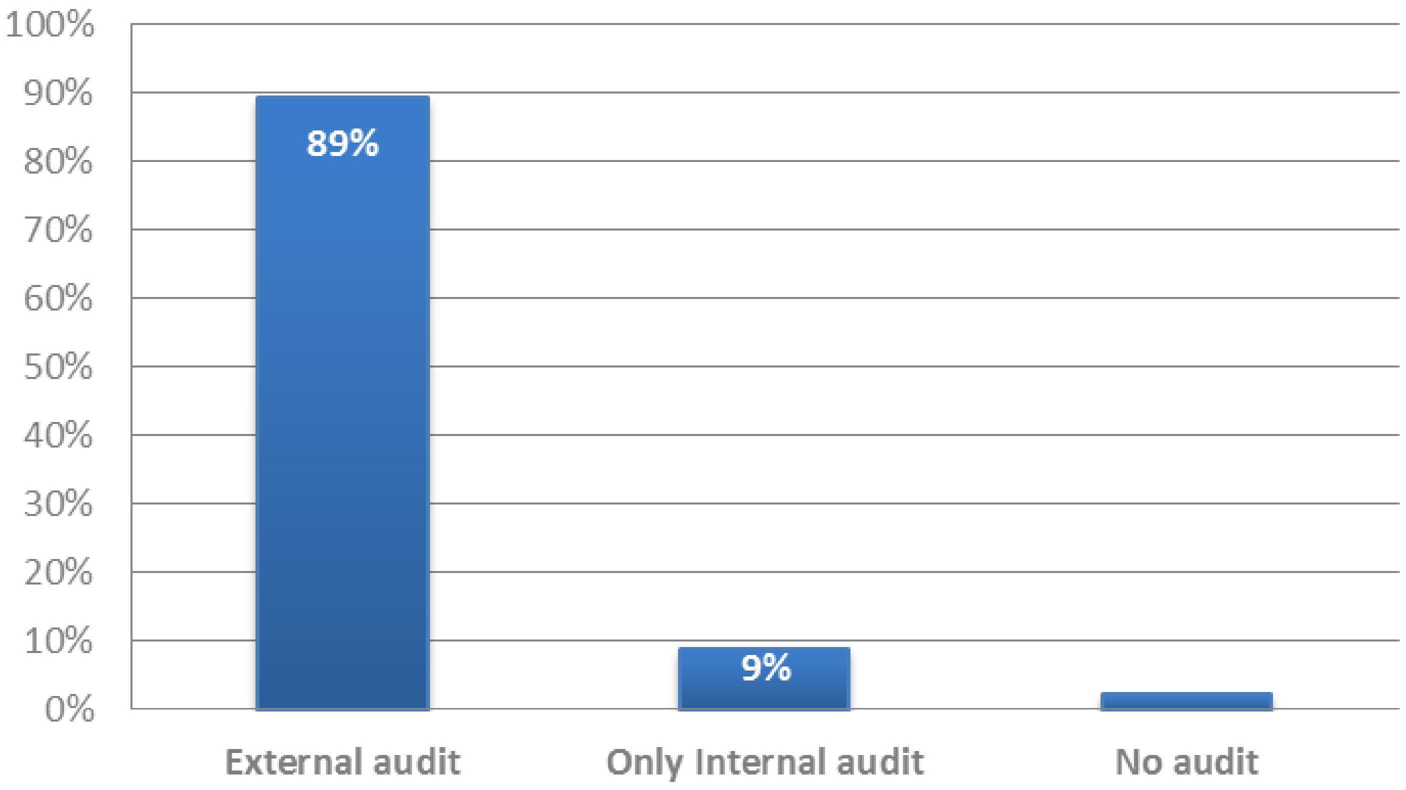
Are the cryptographic modules for CSP signing operations that you use certified against any certification scheme?

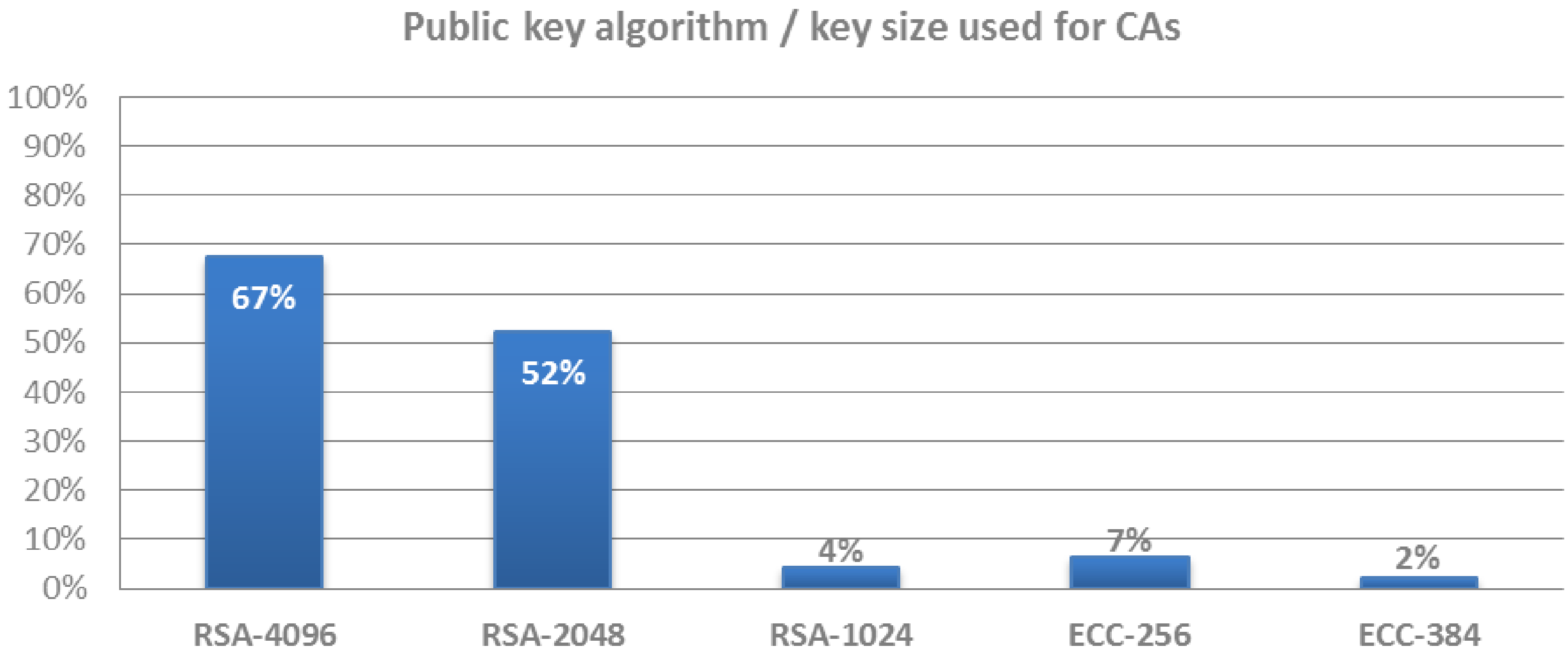


Are the cryptographic modules for subject signing operations that you use certified against any certification scheme?

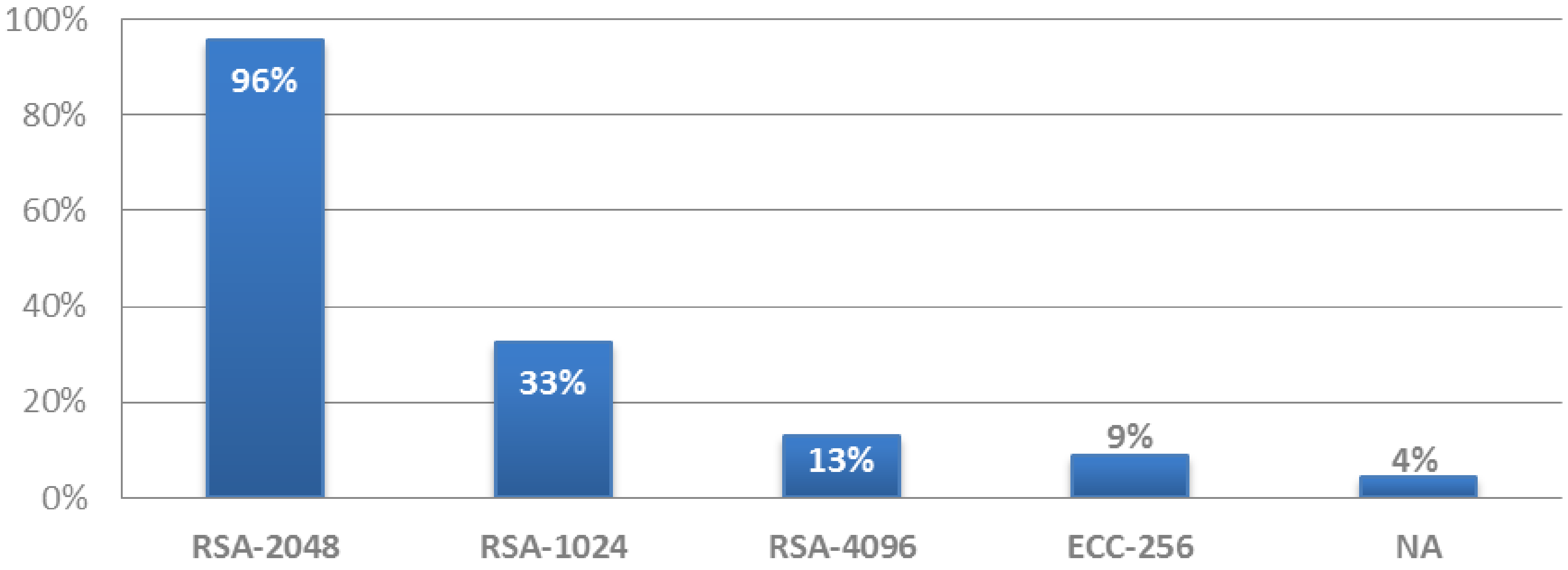


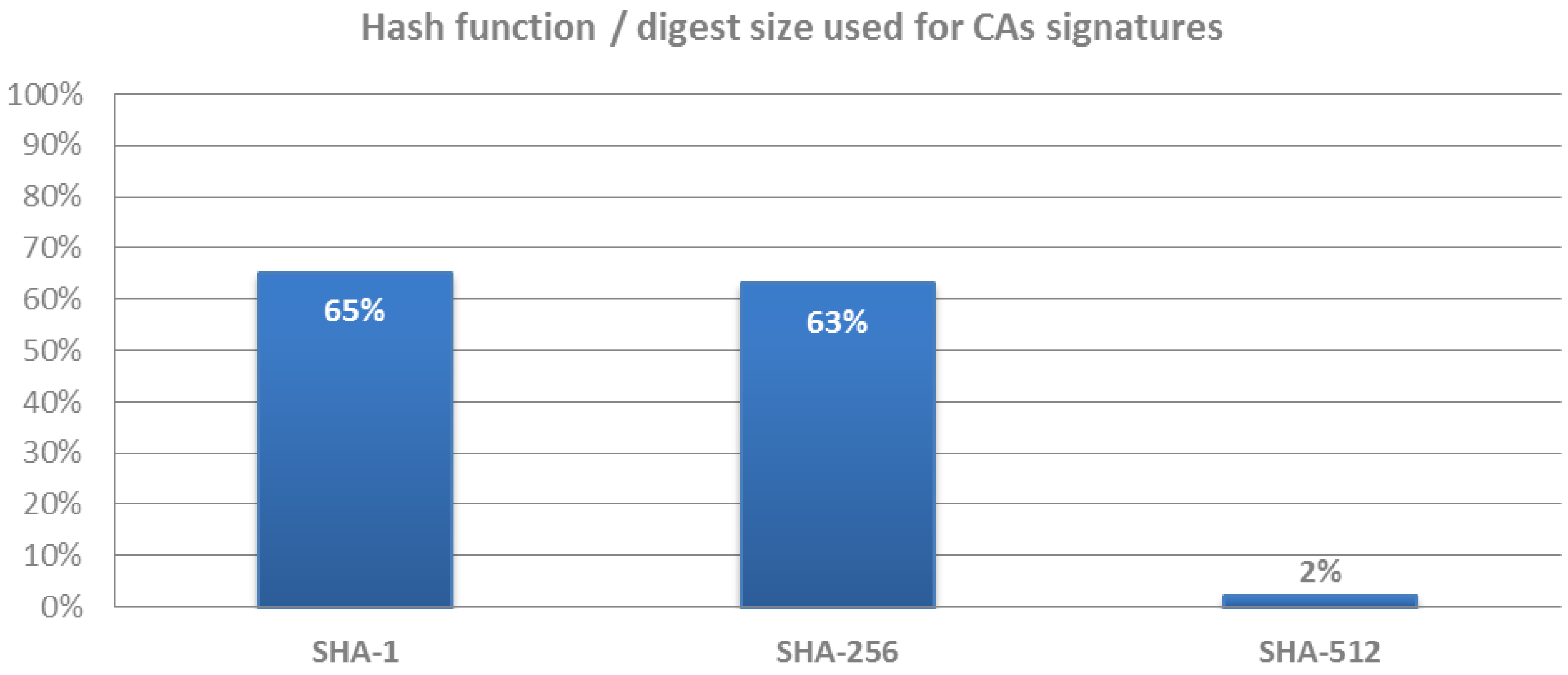
Types of audits CSPs report undergoing:



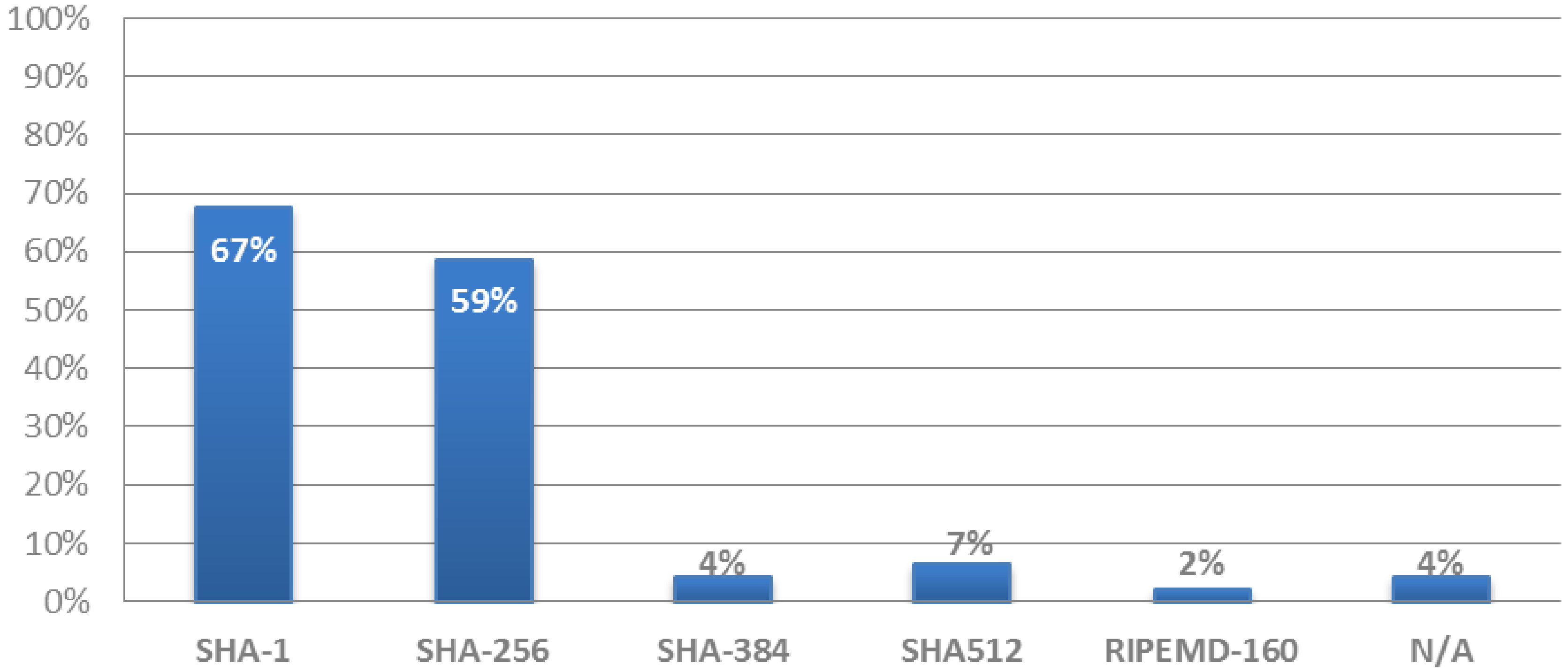

Public key algorithm / key size used for CAs
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
67%
52%
4%
7%
2%
RSA-4096
RSA-2048
RSA-1024
ECC-256
ECC-384

Public key algorithm / key size used for subjects




Hash function / digest size used for CAs signatures
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
65%
63%
2%
SHA-1
SHA-256
SHA-512

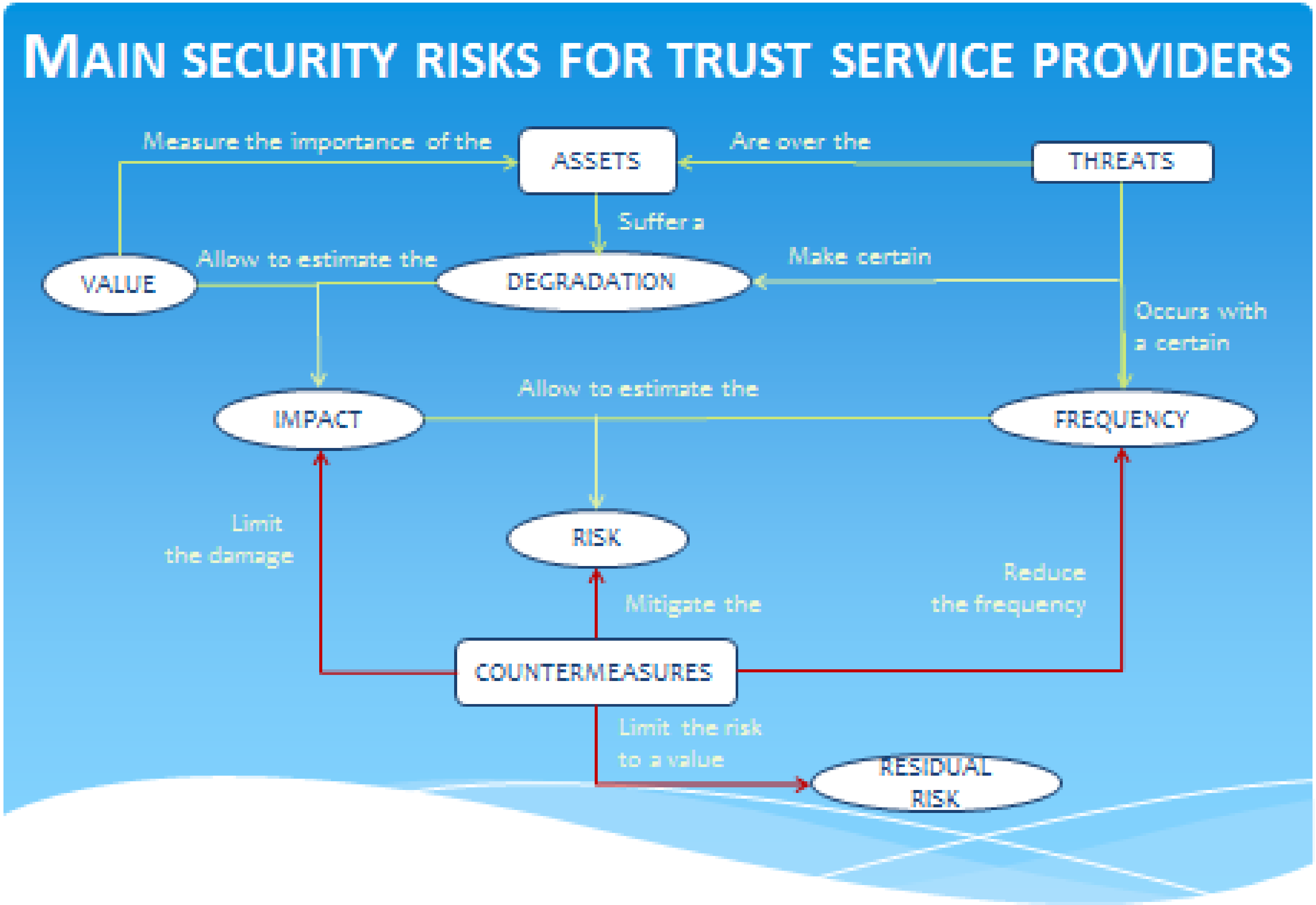
Hash function / digest size used for subject signatures



Panel discussion

- Nick Pope (Thales / ETSI)
- Ben Wilson (DigiCert)

MAIN SECURITY RISKS FOR TRUST SERVICE PROVIDERS



MAIN SECURITY RISKS FOR TRUST SERVICE PROVIDERS

ASSETS

THREATS

VALUE

DEGRADATION

IMPACT

FREQUENCY

RISK

COUNTERMEASURES

RESIDUAL RISK

Measure the importance of the

Are over the

Suffer a

Allow to estimate the

Make certain

Occurs with a certain

Allow to estimate the

Limit the damage

Mitigate the

Reduce the frequency

Limit the risk to a value

Risk management and TSPs

- **Identification of assets**
  - Classification
  - Registration
- **Risk analysis**
  - Value criteria
  - Asset evaluation
  - Risk evaluation
  - Risk threshold level
- **Risk management**
  - Risk acceptance
  - Risk treatment
- **Risk assessment for TSPs**
  - Risk identification
  - Risk analysis
  - Risk evaluation

TSP infrastructure

- **Involved entities**
  - Certificate Authority
  - Registration Authority
  - Subject
  - Relying Party
- **Involved processes**
  - Registration
  - CA key management
  - Subject certificate management
  - Revocation
- **Assets**
  - Primary assets – information, business processes
  - Supporting assets – SW, HW, sites, staff, reputation..

Identify threats

- **Natural hazards**
- **‘Essential services’ availability**
- **Human involved threats**
- **Threat agents**
  - Hackers
  - Criminals
  - Intelligence
  - Terrorists
  - Employees

Analyse vulnerabilities

- Registration process
- CA key management
- Subject certificate management
- Vulnerabilities in revocation process
- Vulnerabilities in CA information and communications systems
- Vulnerabilities affecting TSP operation

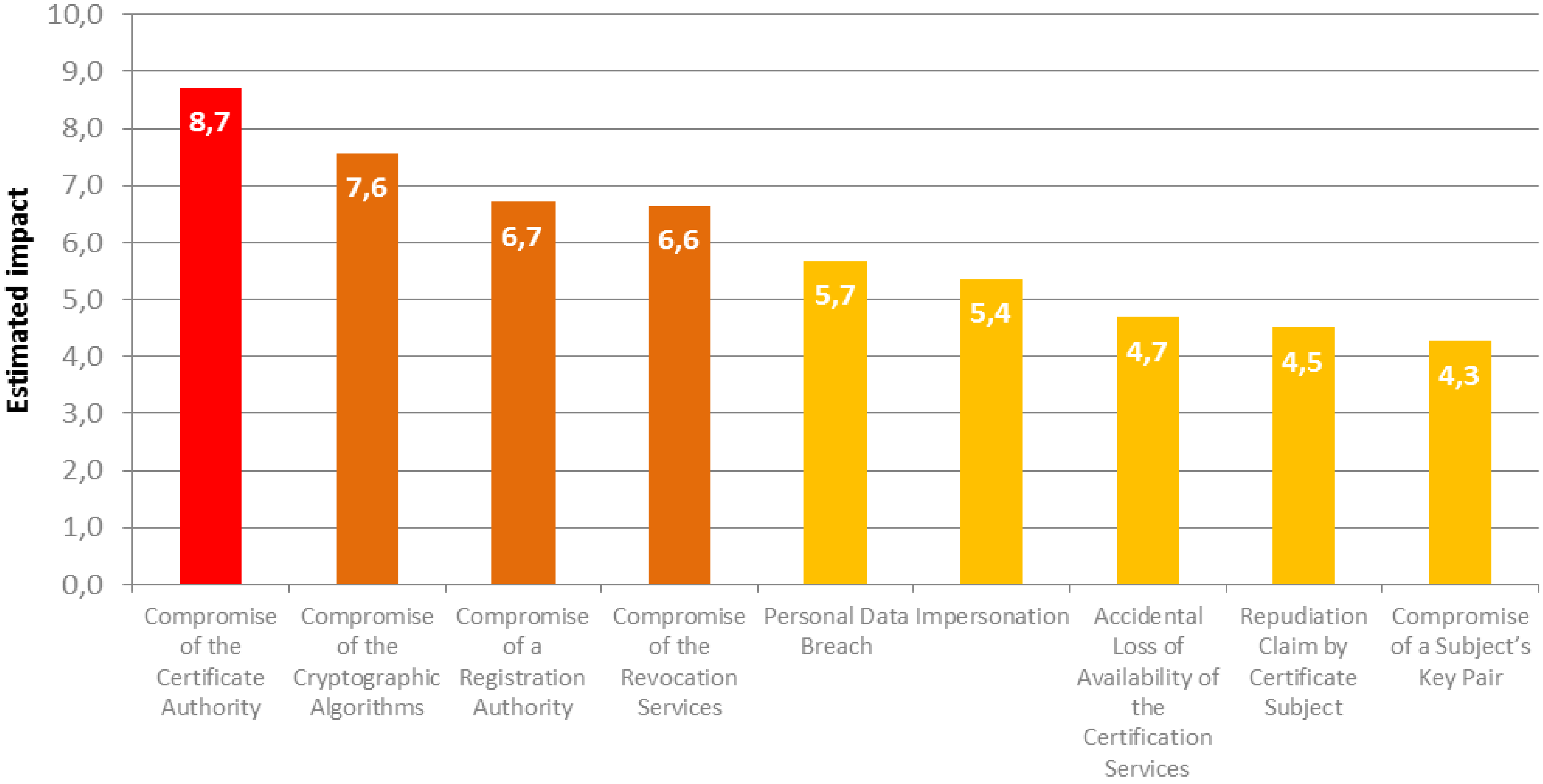
Identifying controls

- Security measures in the registration process
- Security measures in the CA key management lifecycle
- Security measures in the subject certificate management process
- Security measures in the revocation management process
- Security measures in the TSP information and communication system
- Security measures in the TSP operation
- Determine consequences

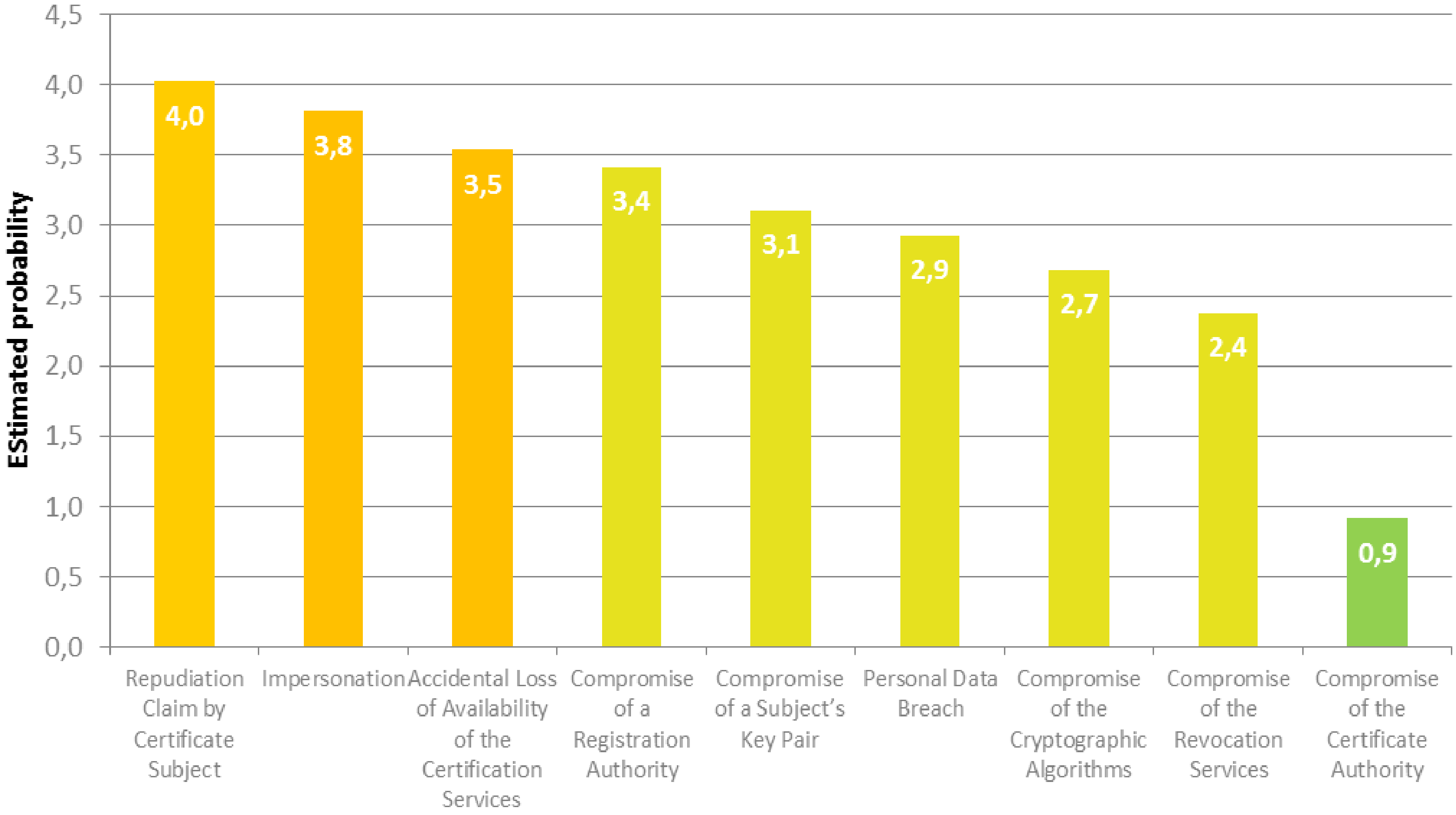
Identifying incident scenarios

- Incidents affecting CAs
- Incidents affecting RAs
- Incidents affecting the subject certificate

Level of impact estimation



Risk probability estimation



Panel discussion

- Kim Nguyen (Bundesdruckerei / D-Trust)
- Audun Jøsang (University of Oslo)
- Iñigo Barreira (Izenpe)

SECURITY ASPECTS OF THE NEW TRUST SERVICES DEFINED IN THE DRAFT REGULATION

MITIGATING THE IMPACT OF SECURITY INCIDENTS IN TRUST SERVICES PROVIDERS

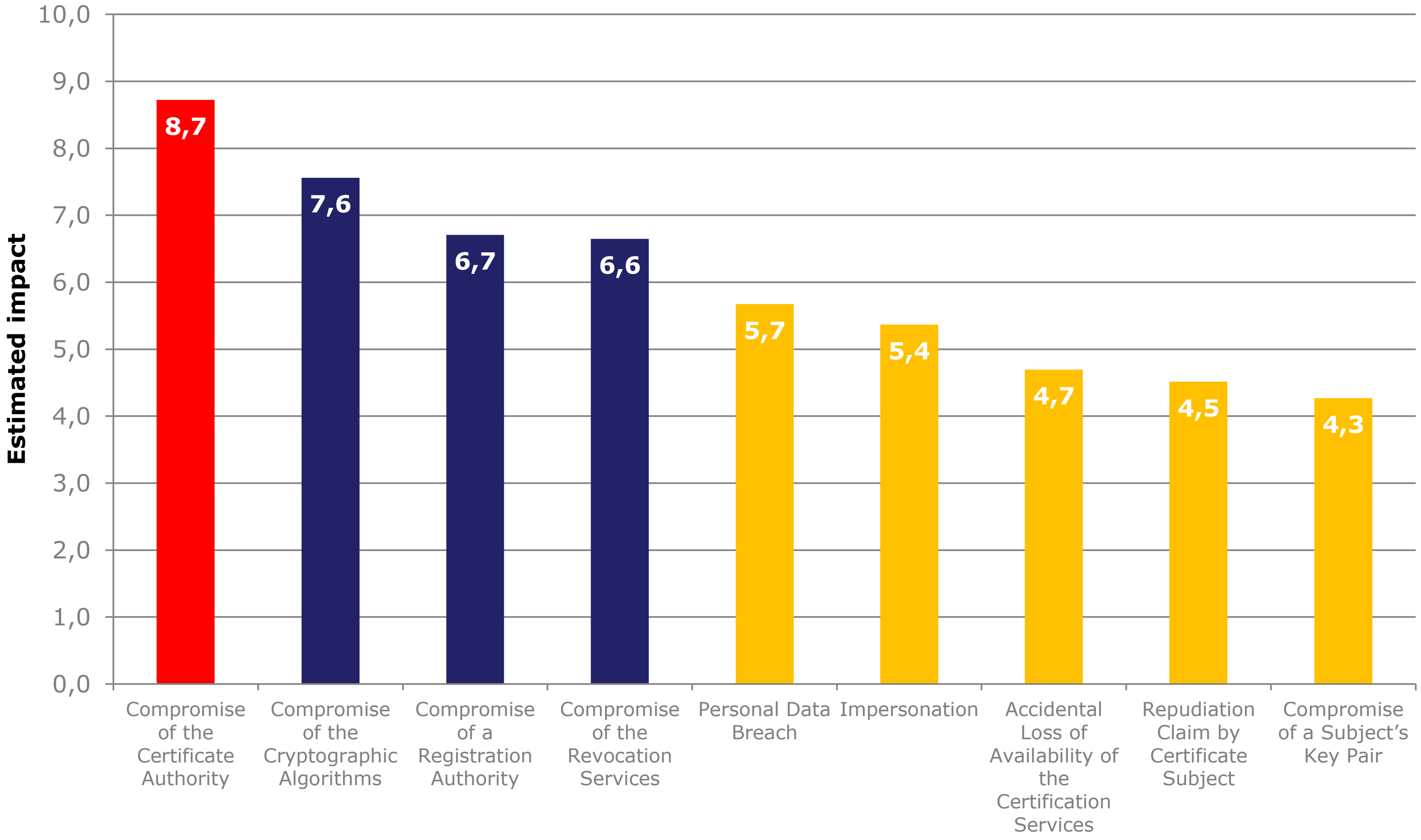
Processes involved in certificate services

- Certification
- CA key management
- Subject key / certificate management
- Revocation

Incident scenarios

- Compromise of a CA
- Compromise of a RA
- Compromise of revocation services
- Compromise of cryptographic modules
- Repudiation claim by certificate subject
- Loss of availability of the certificate
- Compromise of a subject’s private key
- Impersonation
- Personal data breach

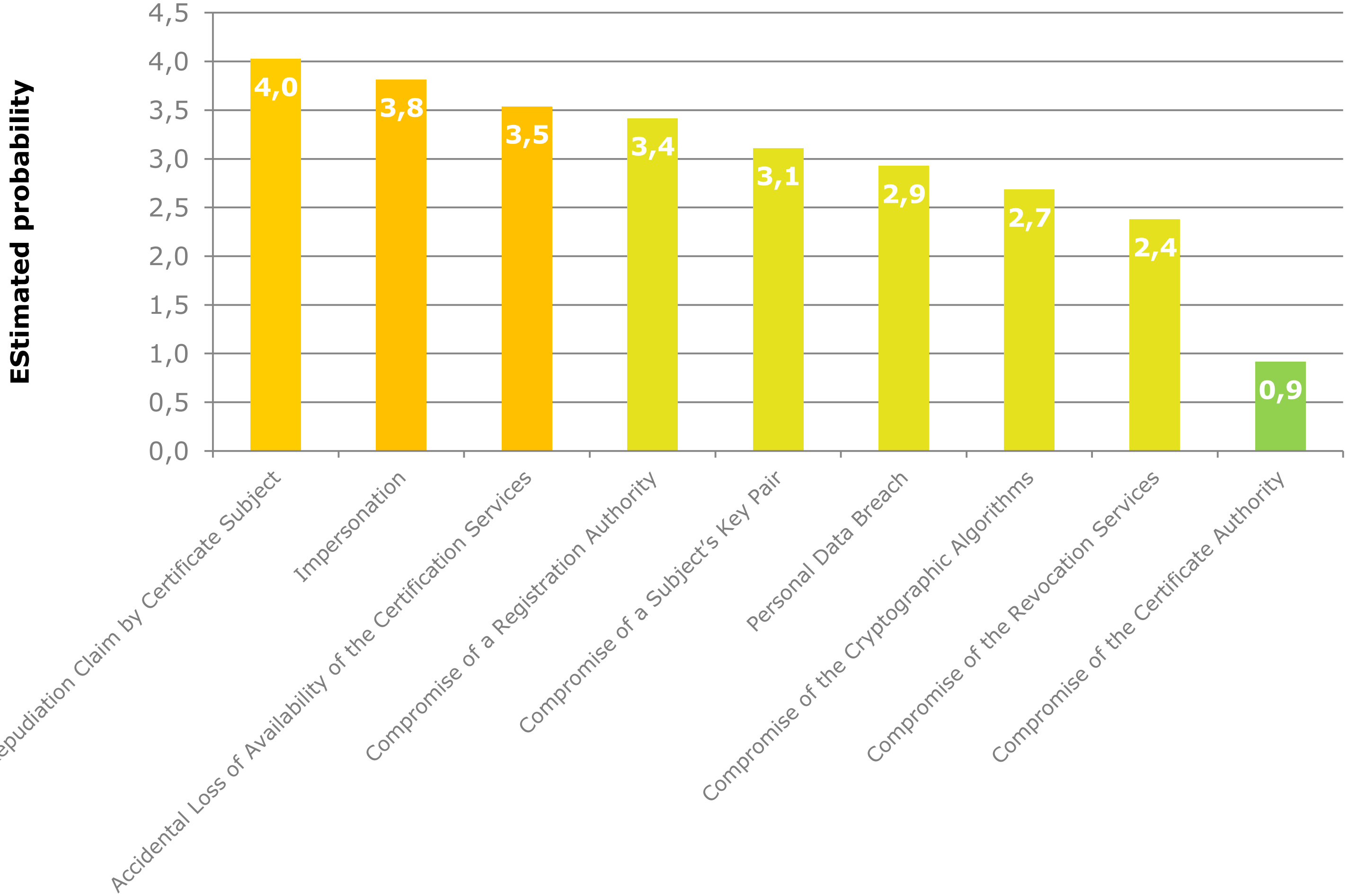
Impact of incidents



Attack vectors

- **Logical attacks**
- **Cryptographic attacks**
- **Insider attacks**
- **Physical attacks**

Probability of occurrence of attack vectors



Preparing for incidents

- Enable means to collect alerts
- Create an incident response capability
- Prepare staff and systems for incidents
- Enable communication means
- Prepare contingency plans

Incident handling

- CA compromise
- RA compromise
- Revocation services compromise
- Cryptographic modules compromise
- Repudiation claim by certificate subject
- Impersonation
- Personal data breach
- Subject’s key pair
- Loss of availability of certificate services

Panel discussion

- **Steve Roylance (GlobalSign)**
- **Robert van de Rijt (Logius)**
- **Christian Van Heurck (CERT.be)**
- **Tomas Gustavsson (PrimeKey Solutions)**

OPEN DISCUSSION & CLOSING REMARKS

European Union Agency for Network and Information Security

Science and Technology Park of Crete

P.O. Box 1309

71001 Heraklion

Crete

Greece

Follow ENISA

http://www.enisa.europa.eu