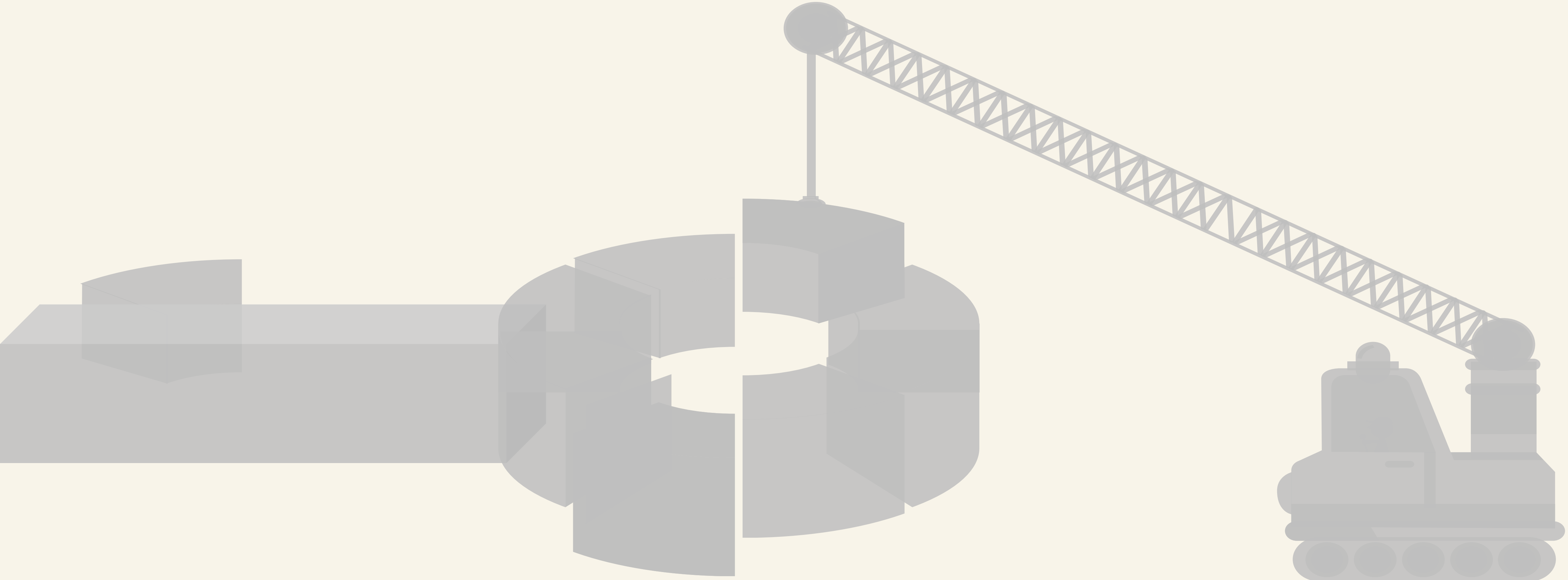
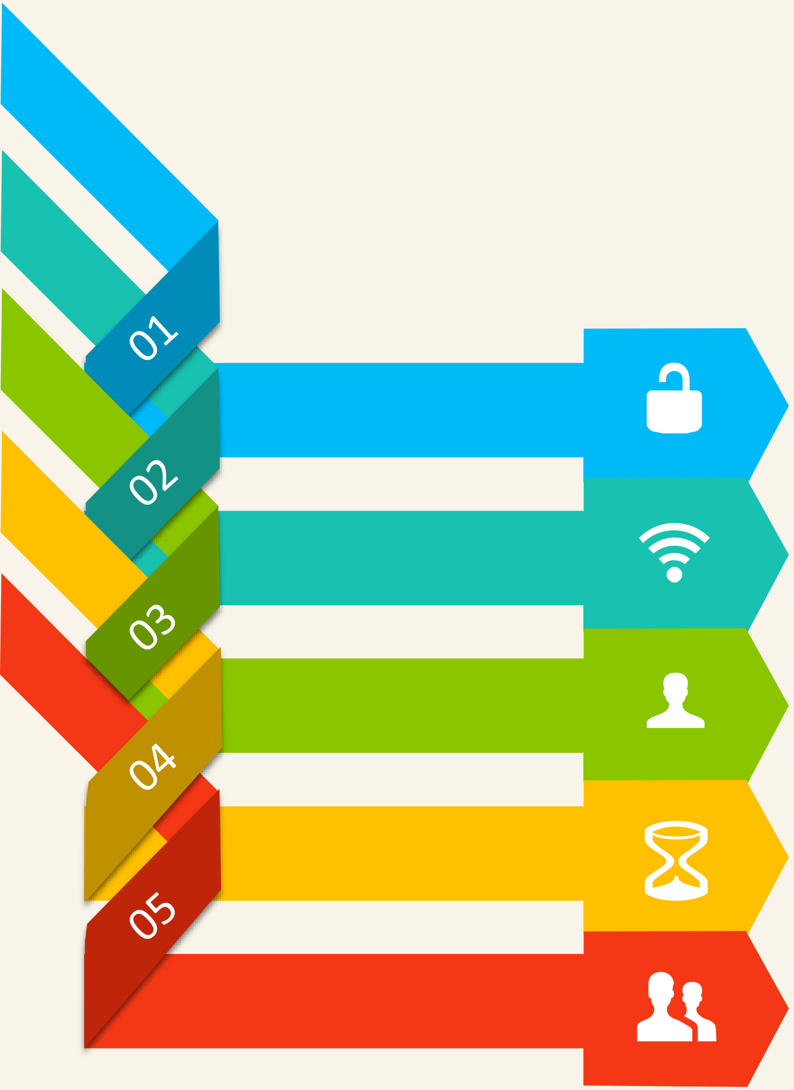
PKI Implementation Roadmap

Dr. Manel Abdelkader, Tunisia

Muscat 11-12/12/17



Need for secure identity management



Increase of identity theft/identity disclosure breaches

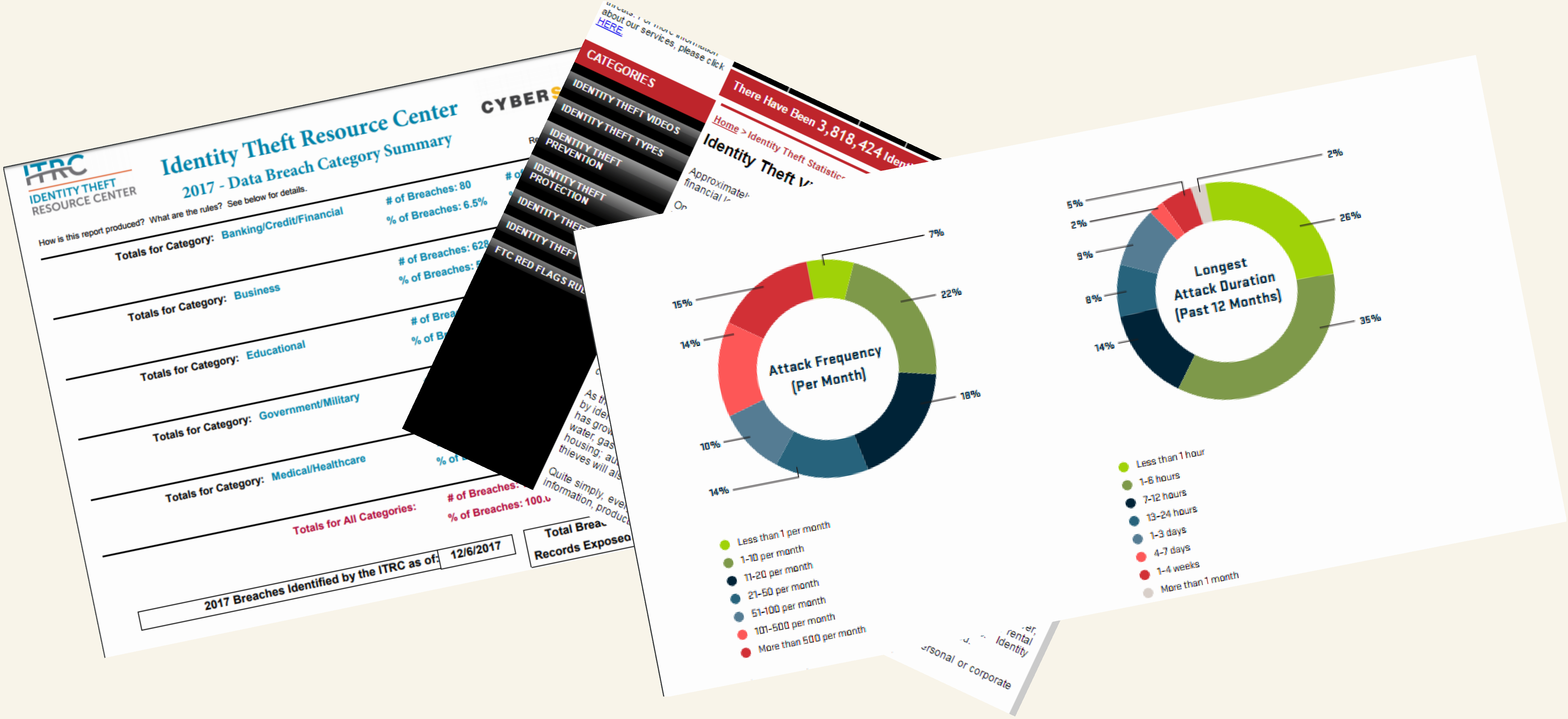
Proliferation of BYOD systems

Evolution of anonymity-preserving tools for the Internet

Extension of the time needed to identify cybercrimes and cyberattacks

Use of multiple identities per user

Identity theft statistics



ITRC IDENTITY THEFT RESOURCE CENTER

Identity Theft Resource Center

2017 - Data Breach Category Summary

How is this report produced? What are the rules? See below for details.

CYBERS

Totals for Category: Banking/Credit/Financial — # of Breaches: 80 — % of Breaches: 6.5%

Totals for Category: Business — # of Breaches: 628 — % of Breaches:

Totals for Category: Educational — # of Brea — % of B

Totals for Category: Government/Military

Totals for Category: Medical/Healthcare — % of

Totals for All Categories: — # of Breaches: — % of Breaches: 100.0

2017 Breaches Identified by the ITRC as of: 12/6/2017

Total Brea

Records Exposed

threats. For more information about our services, please click HERE.

CATEGORIES

IDENTITY THEFT VIDEOS

IDENTITY THEFT TYPES

IDENTITY THEFT PREVENTION

IDENTITY THEFT PROTECTION

IDENTITY THEF

IDENTITY THEFT

FTC RED FLAGS RUL

There Have Been 3,818,424 Iden

Home > Identity Theft Statistics

Identity Theft V

Approximately financial l

On

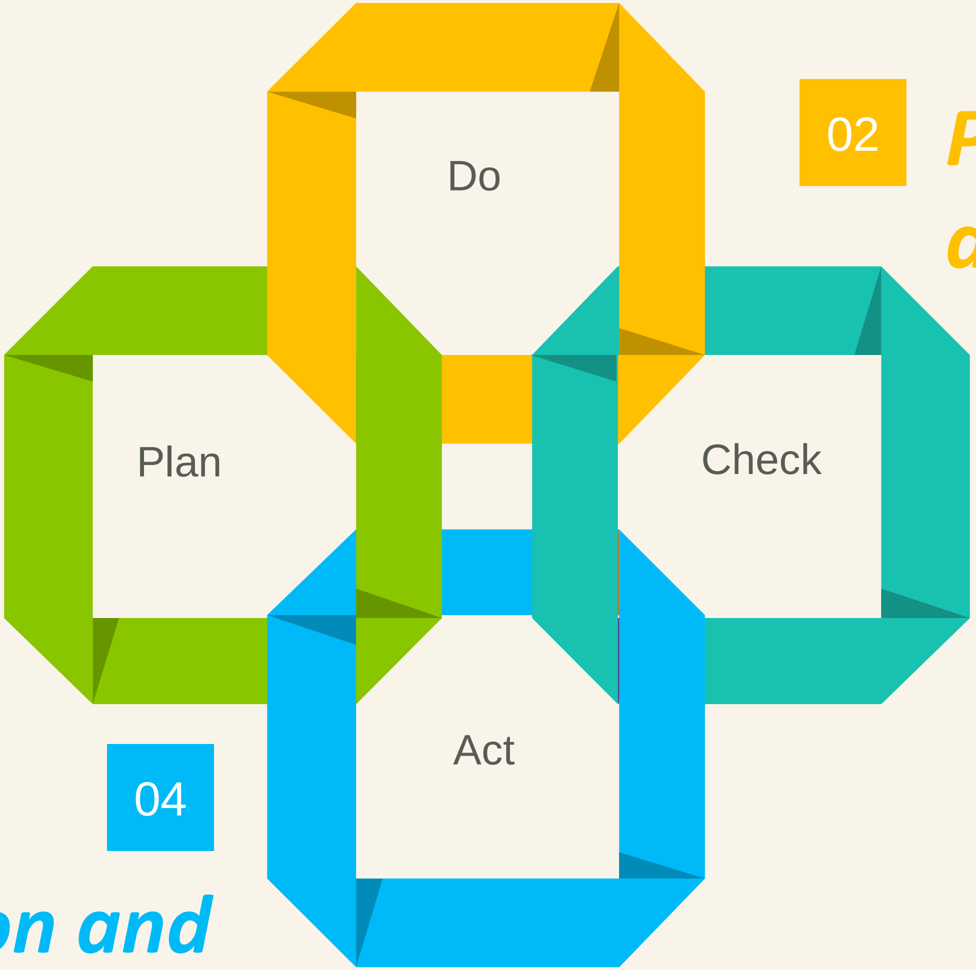
As th by ide has grow water, gas housing; au thieves will als

Quite simply, eve information, produc

er, rental Identity

ersonal or corporate

PKI deployment lifecycle



01 *PKI design*

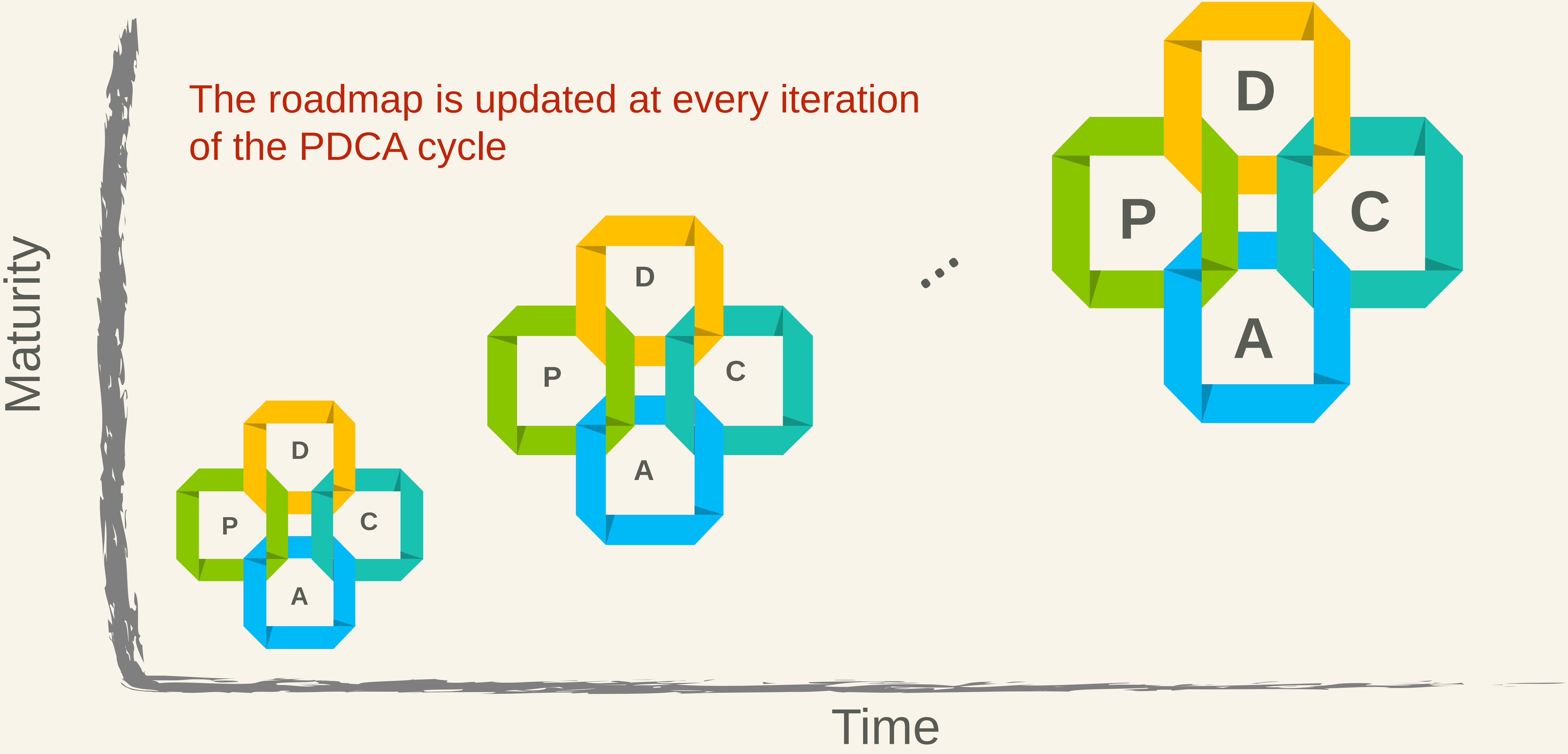
02 *PKI deployment*

03 *PKI evaluation*

04 *Accreditation and recognition*

PKI iterative deployment

The roadmap is updated at every iteration of the PDCA cycle



Plan[1]

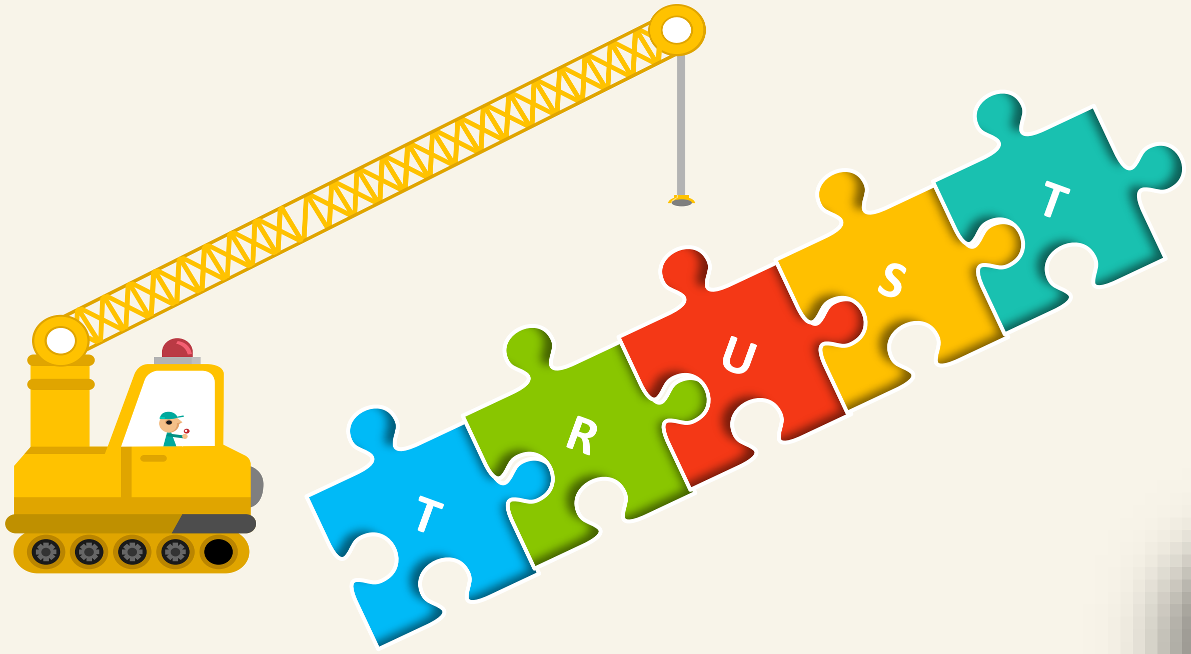
Business requirements analysis

- RoX
- Solutions (existing or need for adaptation?)

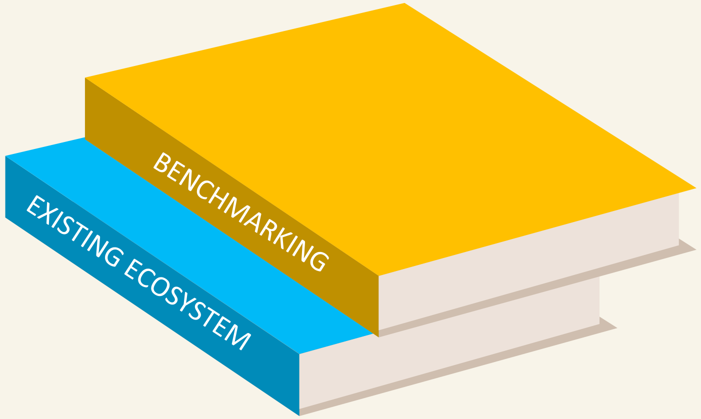
Context analysis

- Regulatory compliance
- Partner compliance
- Customer compliance
- Competitive compliance

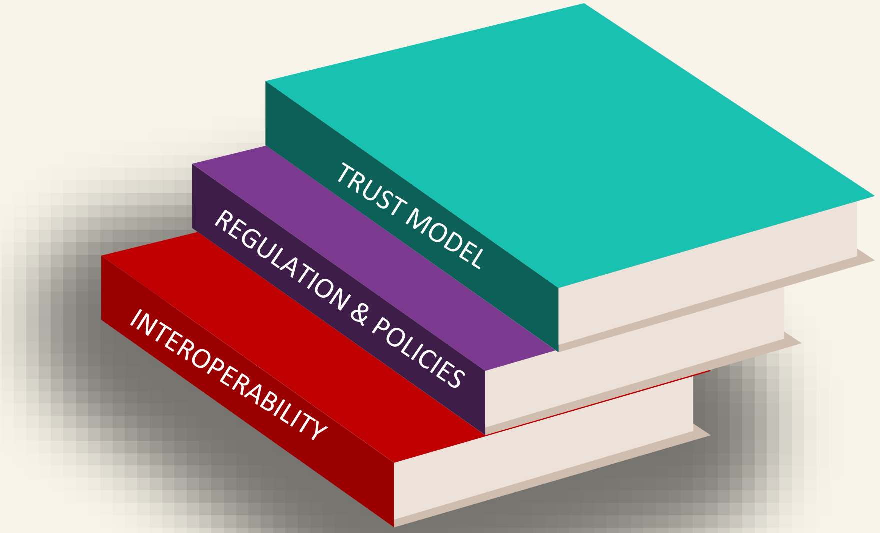
Plan^2



PKI survey and assessment



Defining PKI Architecture



Do

Planning & process design

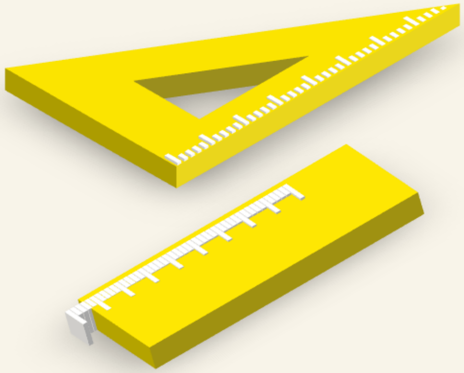
Physical security

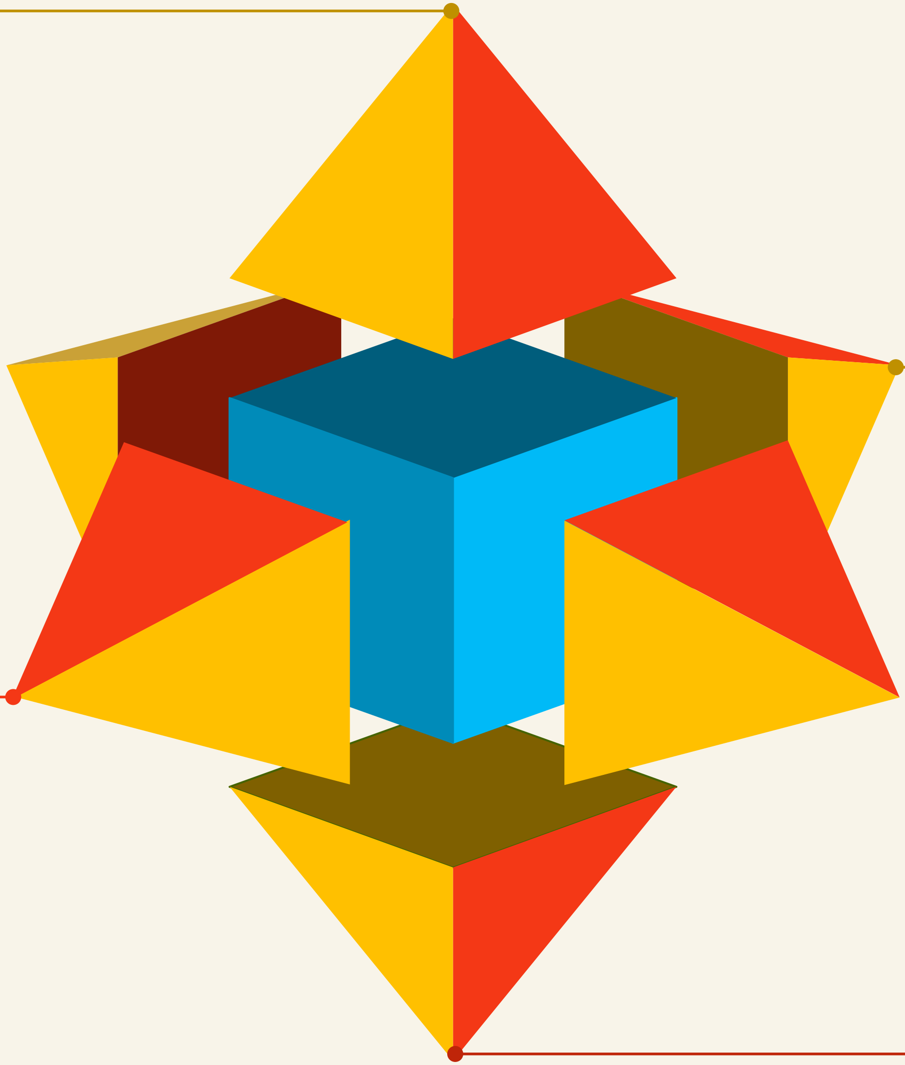
CPS & operational manuals

HR recruitment & capacity building

H&S platforms

Check





Testing

Testing PKI components
Path validation
(NIST project)

Interoperability

Software libraries
APIs

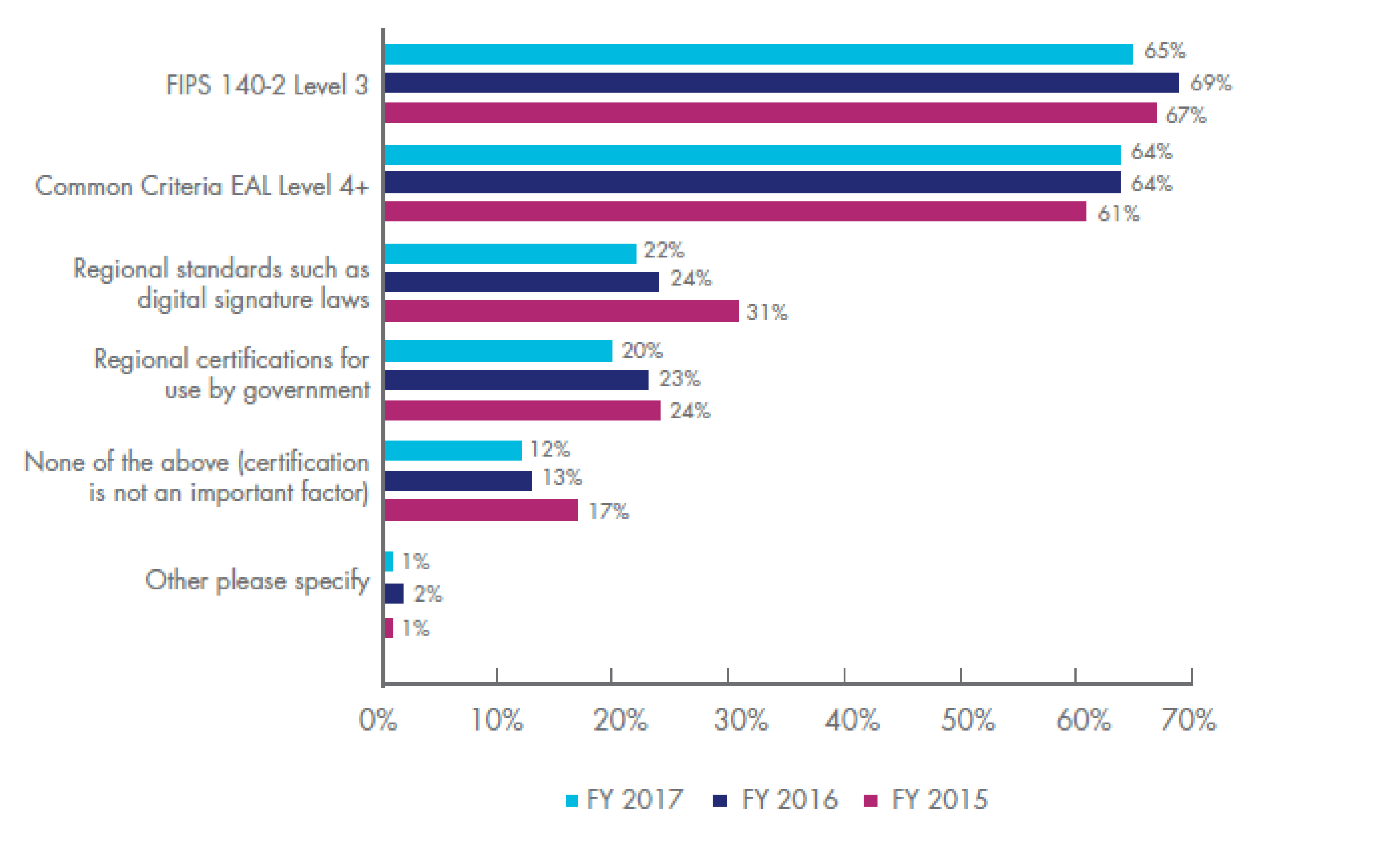
Accreditation

WEBTRUST
ETSI TS 102 042

Intelligence

Key length
Deployment
(managed/In-house)

PKI assessment: standards



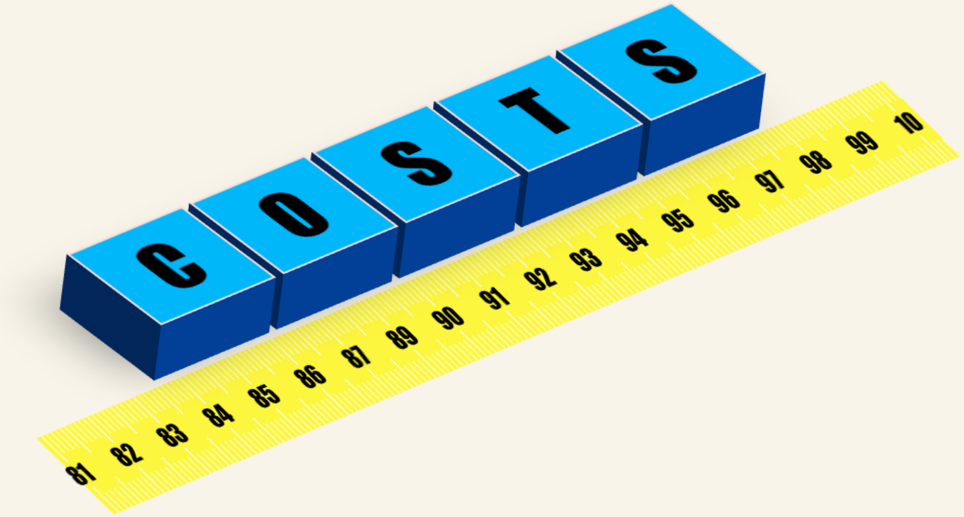
THALES

Ponemon Institute

2017 PKI GLOBAL TRENDS STUDY

October 2017

How to assess PKI costs?



HARDWARE

Servers
HSMS
Smartcards

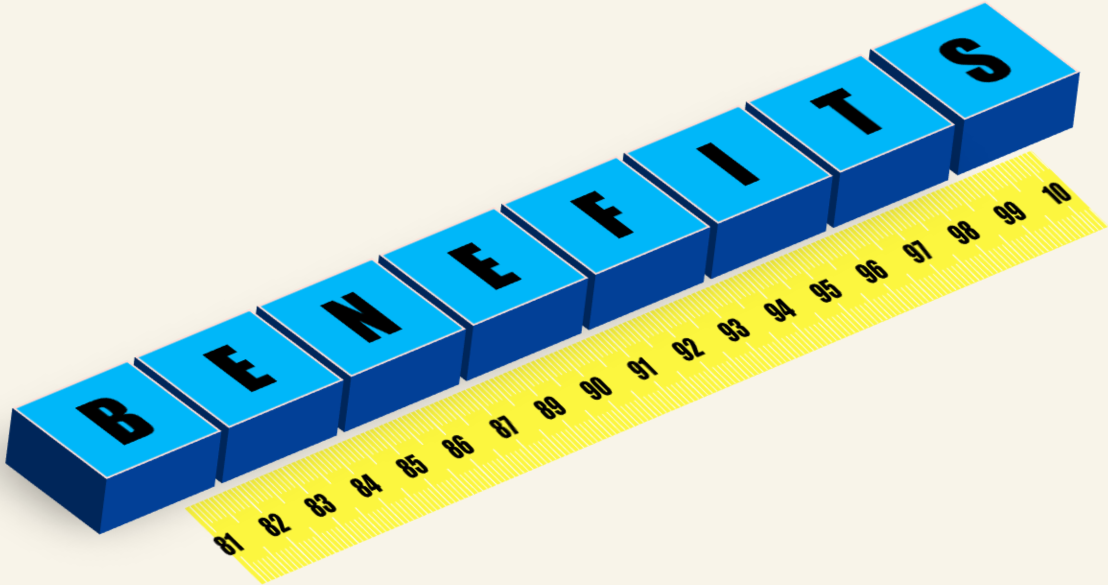
SOFTWARE

CA
CRL, OCSP
Client signature

MANPOWER

Interfaces between CA modules
In-house development

How to assess PKI revenues?



NUMBER OF NEW CUSTOMERS

Customer registration rate
Churn rate?

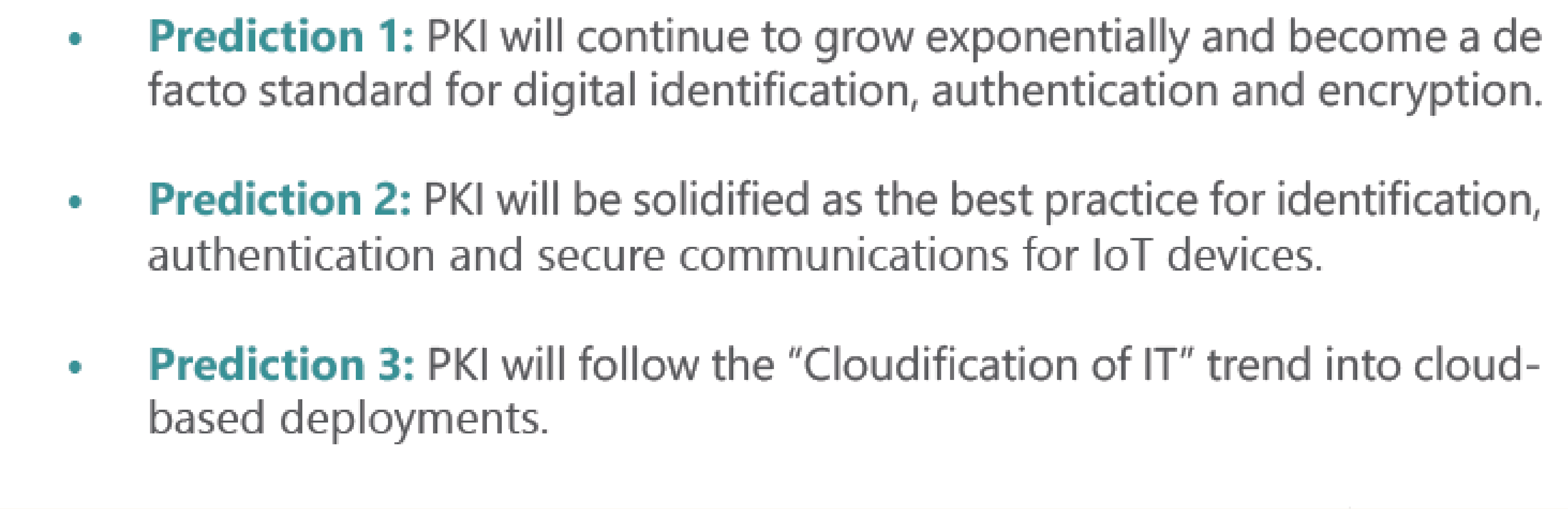
DELAY REDUCTION

Average procesing delay
Time-to-market

THREAT REDUCTION

Number of attack attempts
False positive rate

Future trends



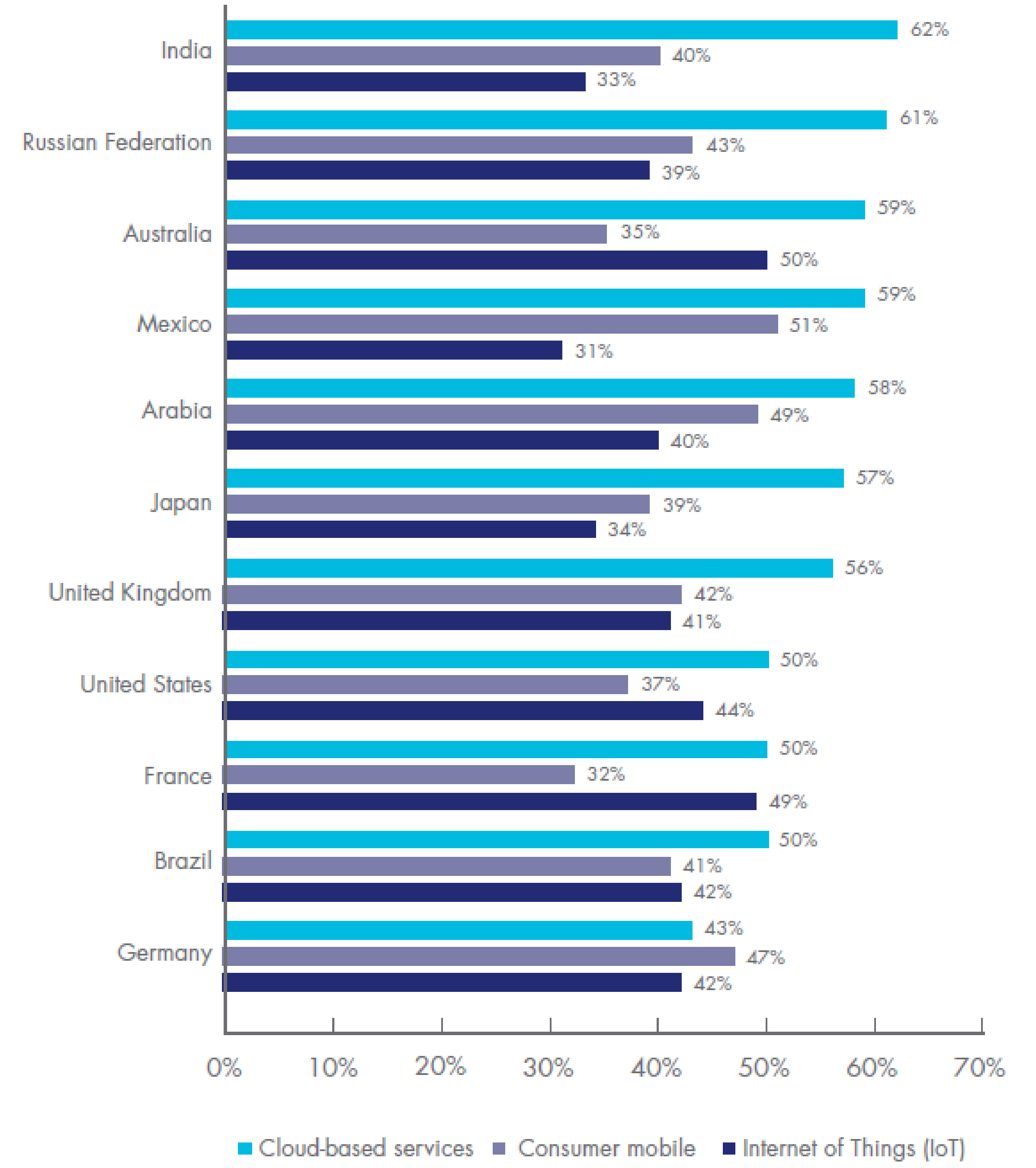
- **Prediction 1:** PKI will continue to grow exponentially and become a de facto standard for digital identification, authentication and encryption.
- **Prediction 2:** PKI will be solidified as the best practice for identification, authentication and secure communications for IoT devices.
- **Prediction 3:** PKI will follow the “Cloudification of IT” trend into cloud-based deployments.

2017 Public Key Infrastructure (PKI) and Internet of Things (IoT) Security Predictions

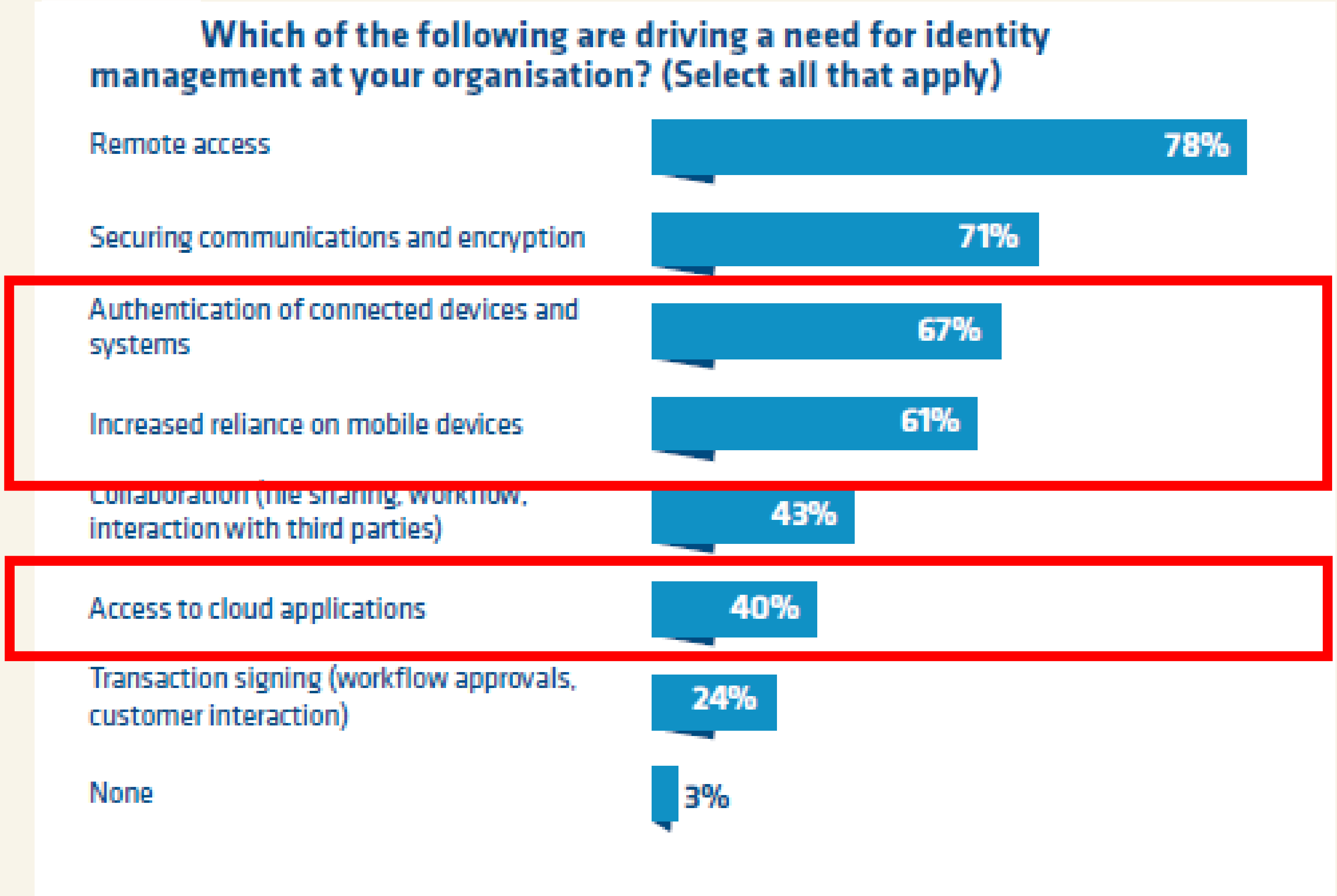
Published by CSS Research I Q1 2017

CSS

What are the most important trends driving the deployment of applications that make use of PKI?



Influence of IoT and Cloud Computing



Which of the following are driving a need for identity management at your organisation? (Select all that apply)

computing research

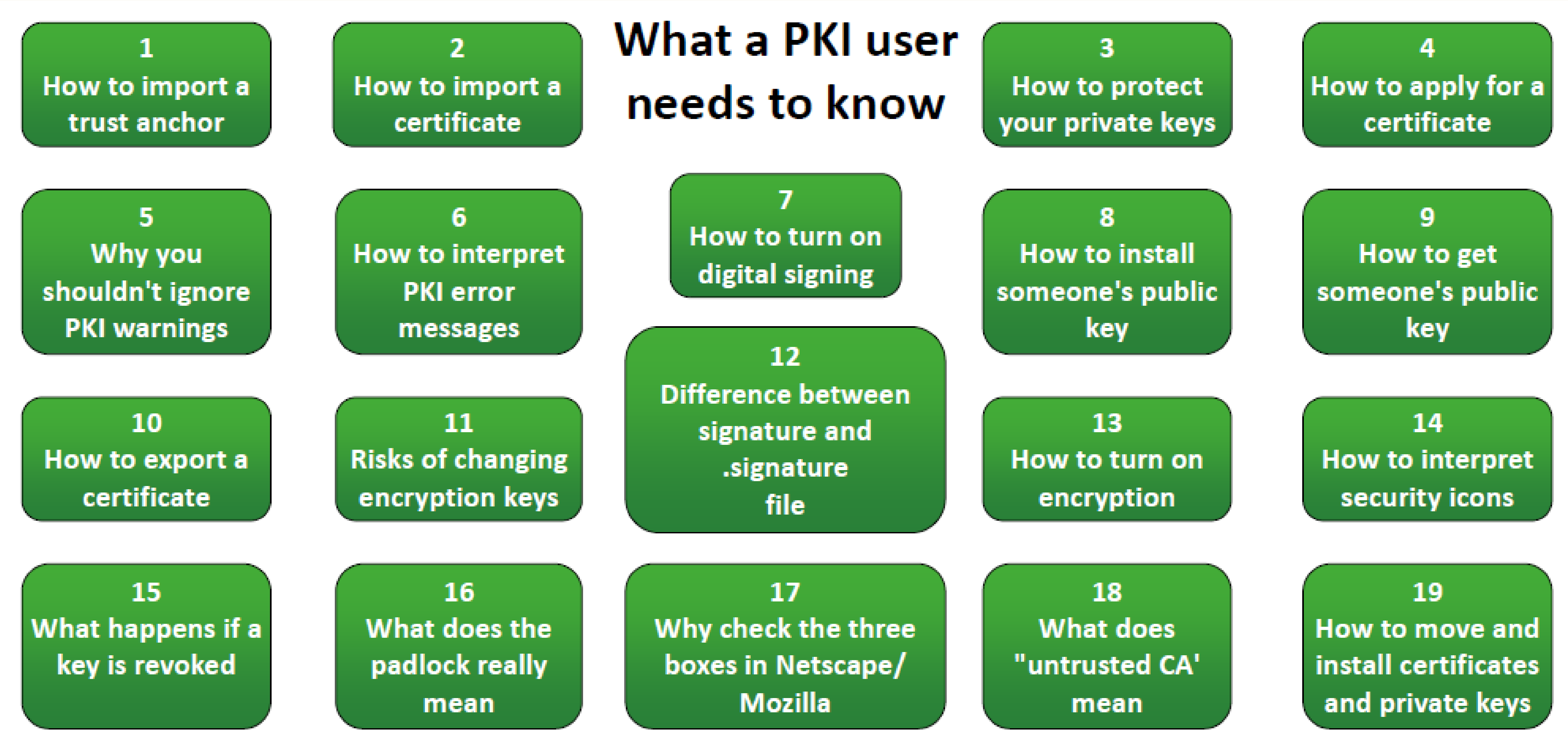
RESEARCH PAPER

Choosing a PKI infrastructure for digital business

Establishing trust to accelerate digital business

June 2017

Sponsored by Entrust Datacard



What a PKI user needs to know

1 How to import a trust anchor

2 How to import a certificate

3 How to protect your private keys

4 How to apply for a certificate

5 Why you shouldn't ignore PKI warnings

6 How to interpret PKI error messages

7 How to turn on digital signing

8 How to install someone's public key

9 How to get someone's public key

10 How to export a certificate

11 Risks of changing encryption keys

12 Difference between signature and .signature file

13 How to turn on encryption

14 How to interpret security icons

15 What happens if a key is revoked

16 What does the padlock really mean

17 Why check the three boxes in Netscape/ Mozilla

18 What does "untrusted CA' mean

19 How to move and install certificates and private keys

Next generation Key Management

- Manage both public and secret (private) keys
- Manage all public keys with the same means
- Maximize flexibility when handling secret keys
- Simplify secret key enrolment and key roll-over
- Consider virtualized scenarios and mobile devices

What a PKI user needs to know

~~1 How to import a trust anchor~~

~~2 How to import a certificate~~

~~3 How to protect your private keys~~

~~4 How to apply for a certificate~~

5 Why you shouldn't ignore PKI warnings

~~6 How to interpret PKI error messages~~

7 How to turn on digital signing

~~8 How to install someone's public key~~

~~9 How to get someone's public key~~

~~10 How to export a certificate~~

~~11 Risks of changing encryption keys~~

~~12 Difference between signature and signature file~~

13 How to turn on encryption

14 How to interpret security icons

~~15 What happens if a key is revoked~~

16 What does the padlock really mean

17 Why check the three boxes in Netscape/ Mozilla

18 What does "untrusted CA' mean

~~19 How to move and install certificates and private keys~~

Proposed Changes in X.509 (2016)

- Cleaning up of the text
  - Removing errors and inconsistencies and replacing badly worded descriptions
- Removing non-PKI and PMI material from X.509
  - Move the directory authentication specifications from X.509 to X.511.
  - Move Password Policy specifications from X.509 to X.511
  - Move Password Policy schema definitions from X.509 to X.520
- Cleanly separate PKI and PMI into different sections
  - In Aug 13 issued a defect report on text which said ACs and PKCs could appear in the same CRL
- Removing unused and duplicate ASN.1 data structures
  - certificationPath, forwardCertificationPath and crossCertificate (pkiPath is used instead)

Open issues

WILL PKI ADAPT TO NEW NETWORKING/COMPUTING PARADIGMS?

CLOUD COMPUTING

New investment models

New governance models

Risk sharing

IoT

No IP addresses

Limited CPU, memory, and storage resources

Dynamic space-time behavior

BIG DATA

Complexity of cryptographic routines

Multiple processing needs (e.g., search, aggregation)

Dramatic increase in size

SOCIAL NETWORKS

New types of communities

New types of threats

THANKS

FOR YOUR ATTENTION