Sultanate of Oman
Information Technology Authority
National Digital Certification Center

Oman National
PKI and Digital Identity

AGENDA

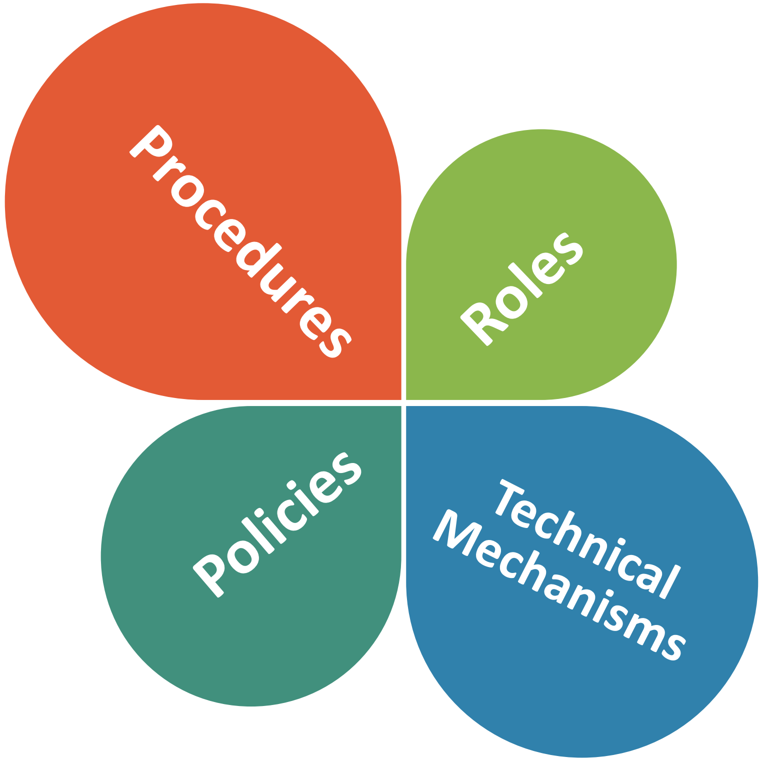
- What is PKI?
- PKI Features
- Trust Services pyramid Components
- Government eServices
- PKI Hierarchy
- PKI implementations
- Who Uses PKI
- Statistics

What is PKI?

Public Key Infrastructure

Set of Roles, Policies, Procedures and Technical Mechanisms to create, manage, distribute and revoke digital certificates.

Provides security services such as strong authentication, integrity, confidentiality and non-repudiation.



What is PKI?

Public Key Infrastructure

- ❑ PKI is security architecture provides an increased level of confidence
- ❑ PKI enables electronic signature for online transactions with non-repudiation
- ❑ PKI leverage Data Protection as it is compliant with e-transaction laws

What is PKI?

Public Key Infrastructure

- PKI enables the exchange information over Internet through the use of public and private cryptographic key pairs

- PKI enables the online service providers to identify and authenticate their clients electronically

OBJECTIVES

1

Protection against Identity Fraud

2

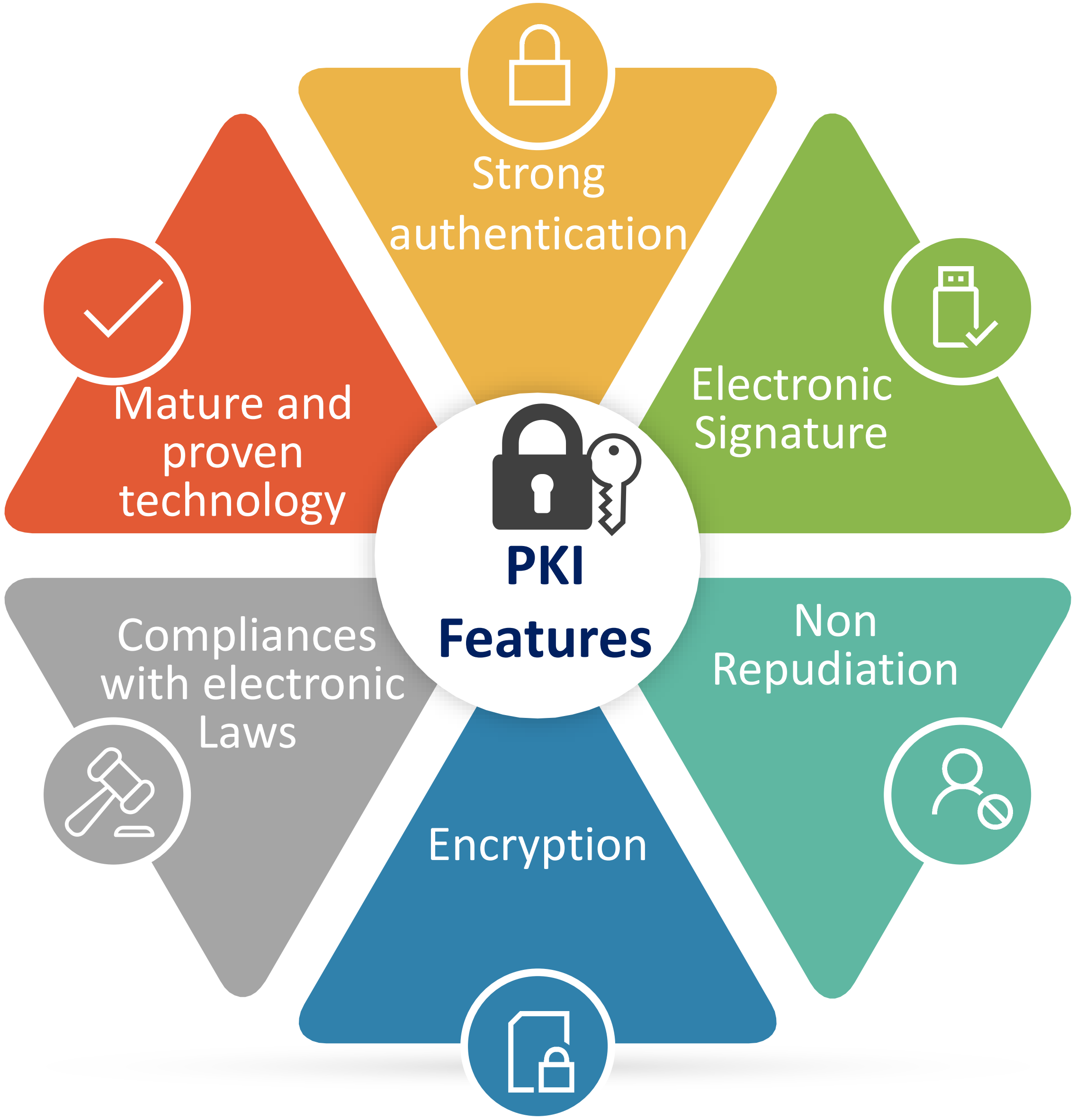
Data Integrity
Data Confidentiality
Strong Authentication
Non Repudiation

3

Trust and Confidence

4

Easing e-services



PKI Features

Strong authentication

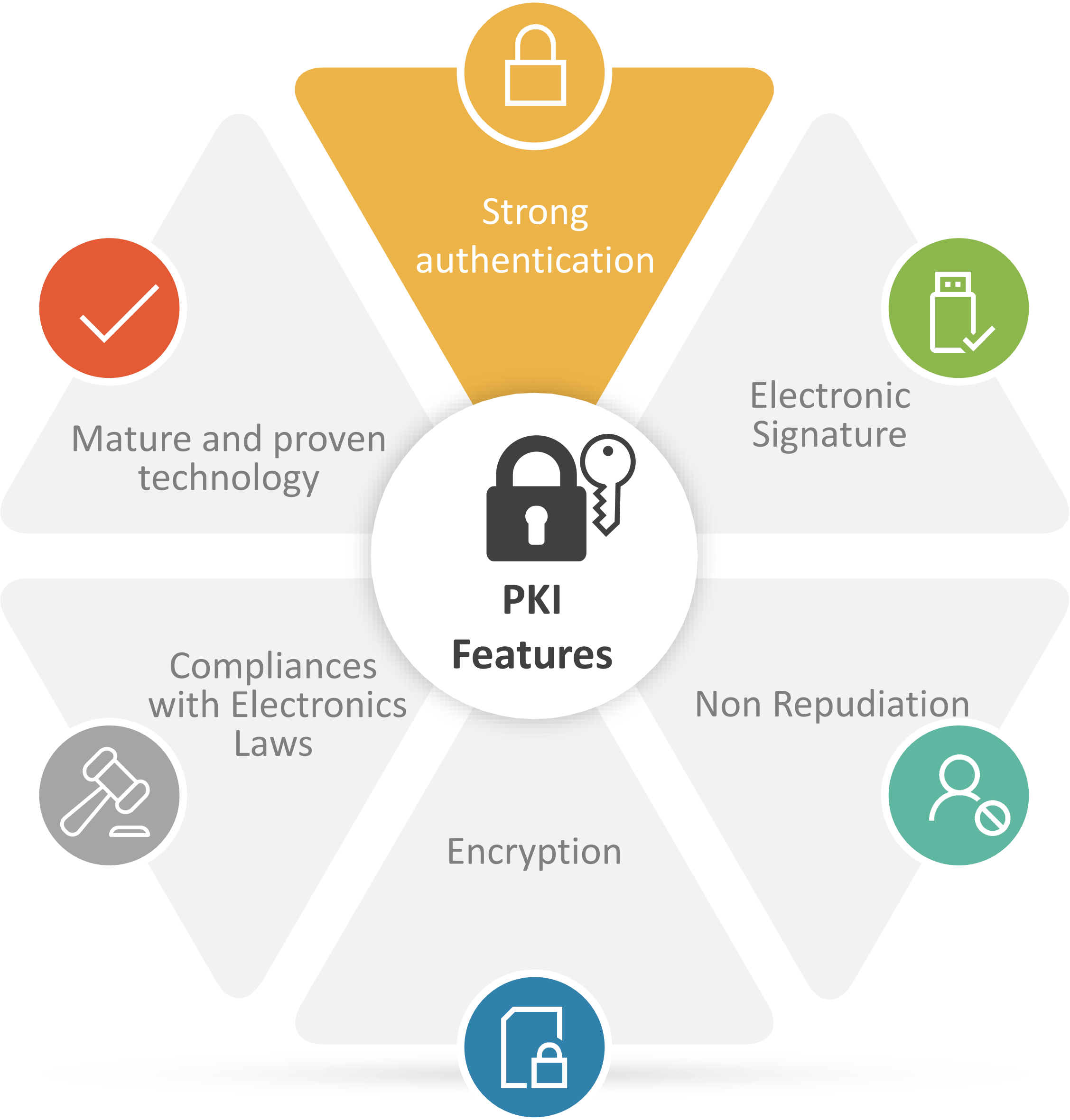
Electronic Signature

Non Repudiation

Encryption

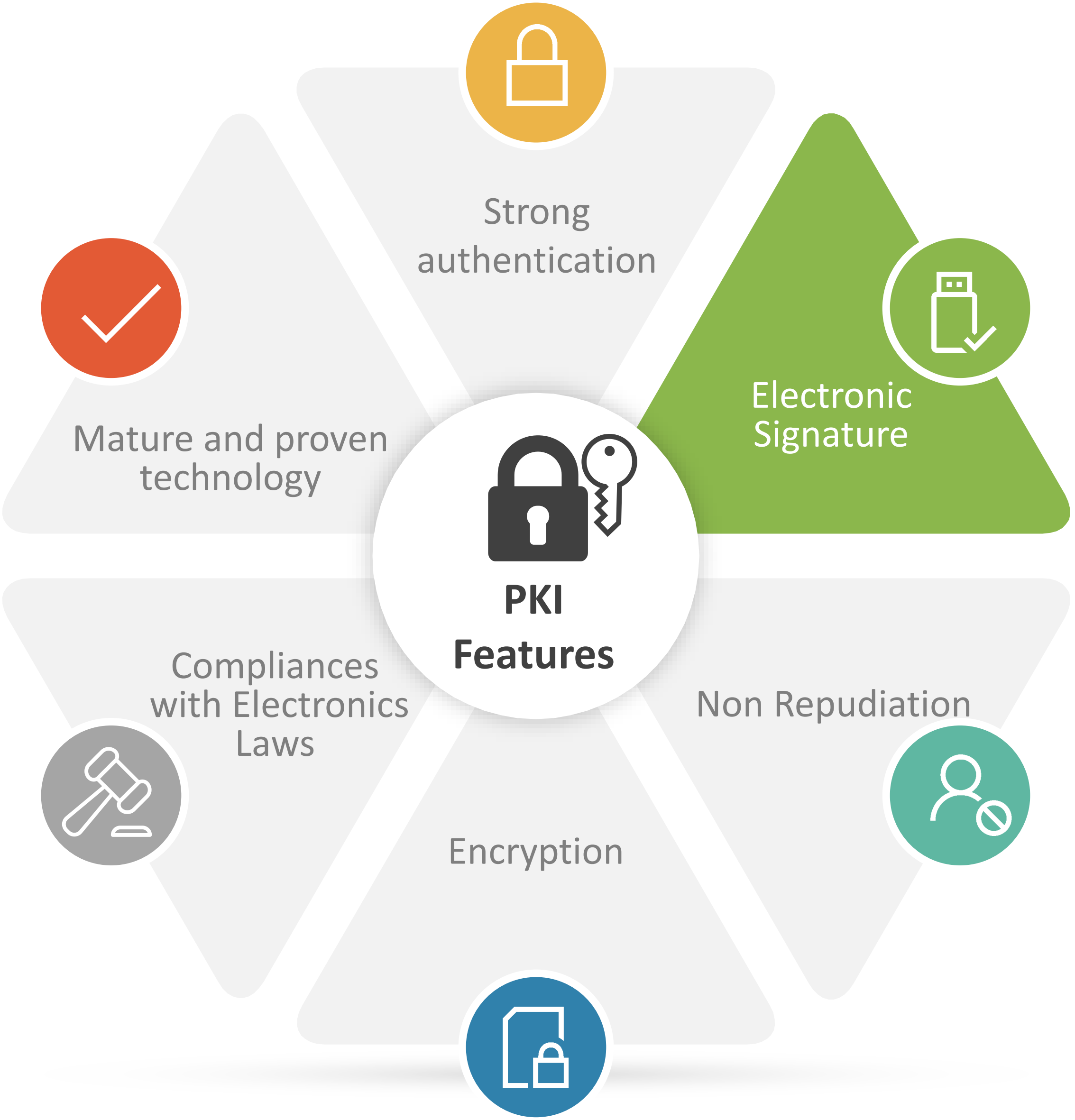
Compliances with electronic Laws

Mature and proven technology



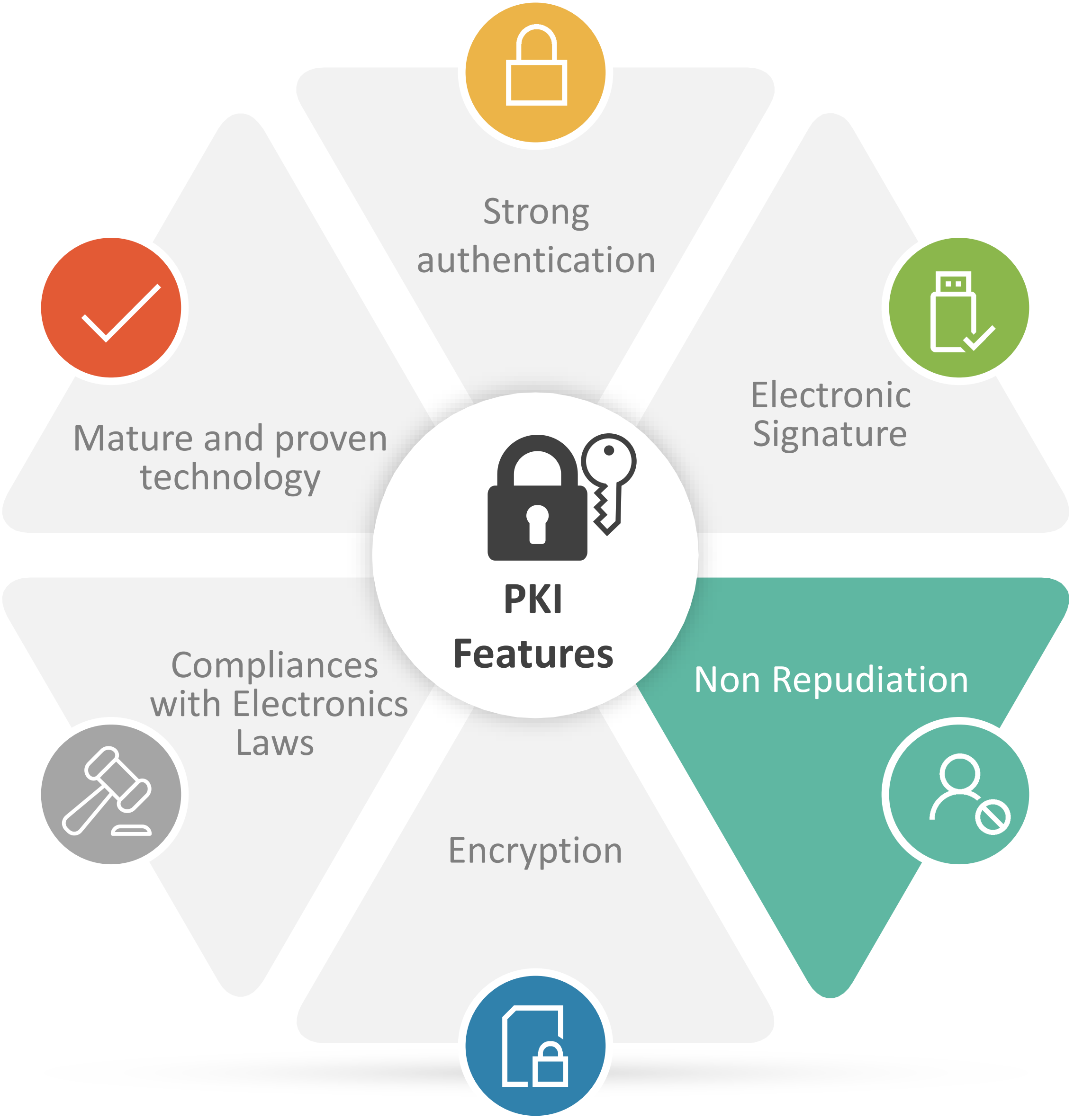
Two Factor Authentication

Two Factor authentication for Government and Private Portals and mobile apps



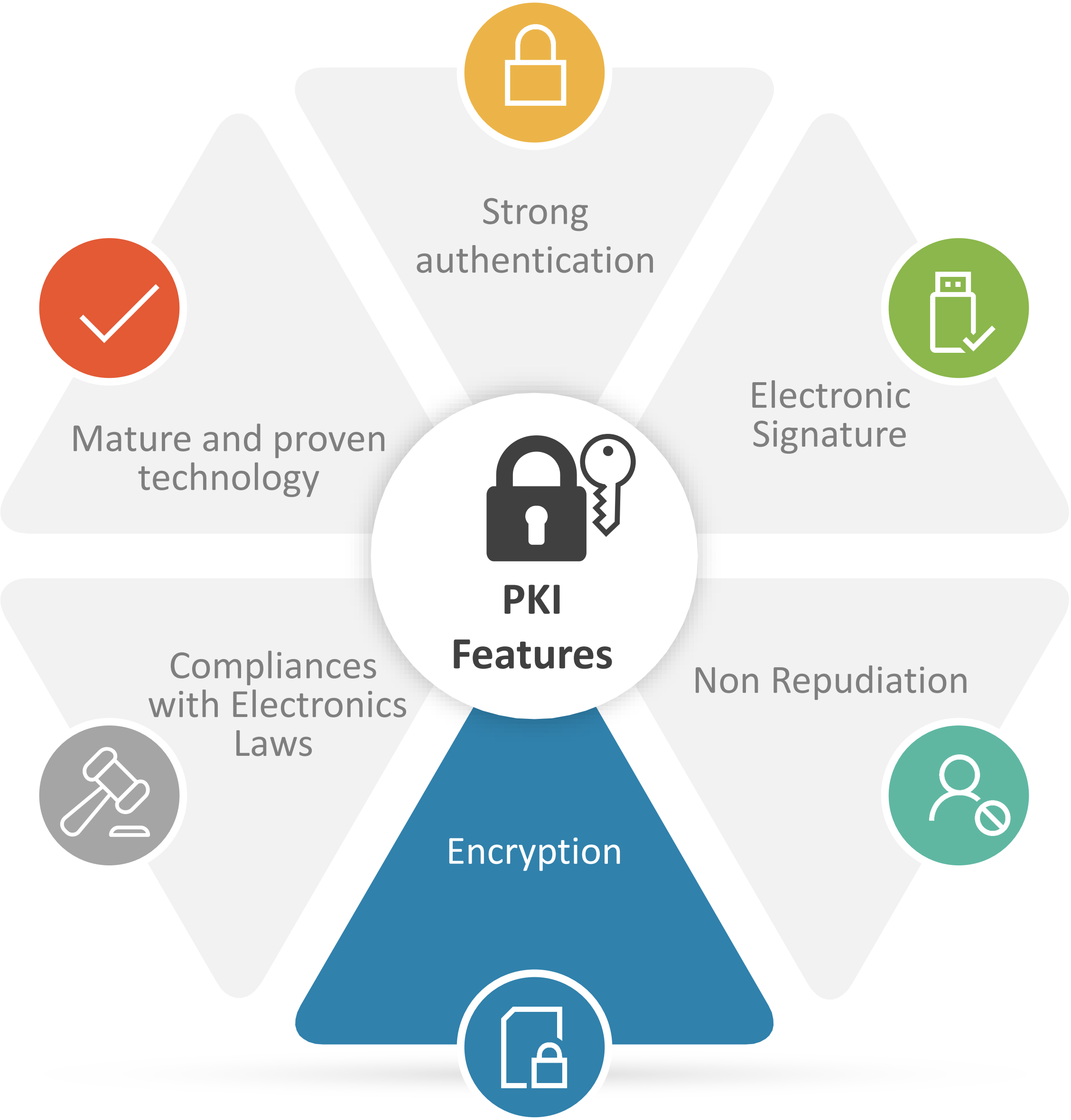
Electronic Signature

using private keys securing the data integrity



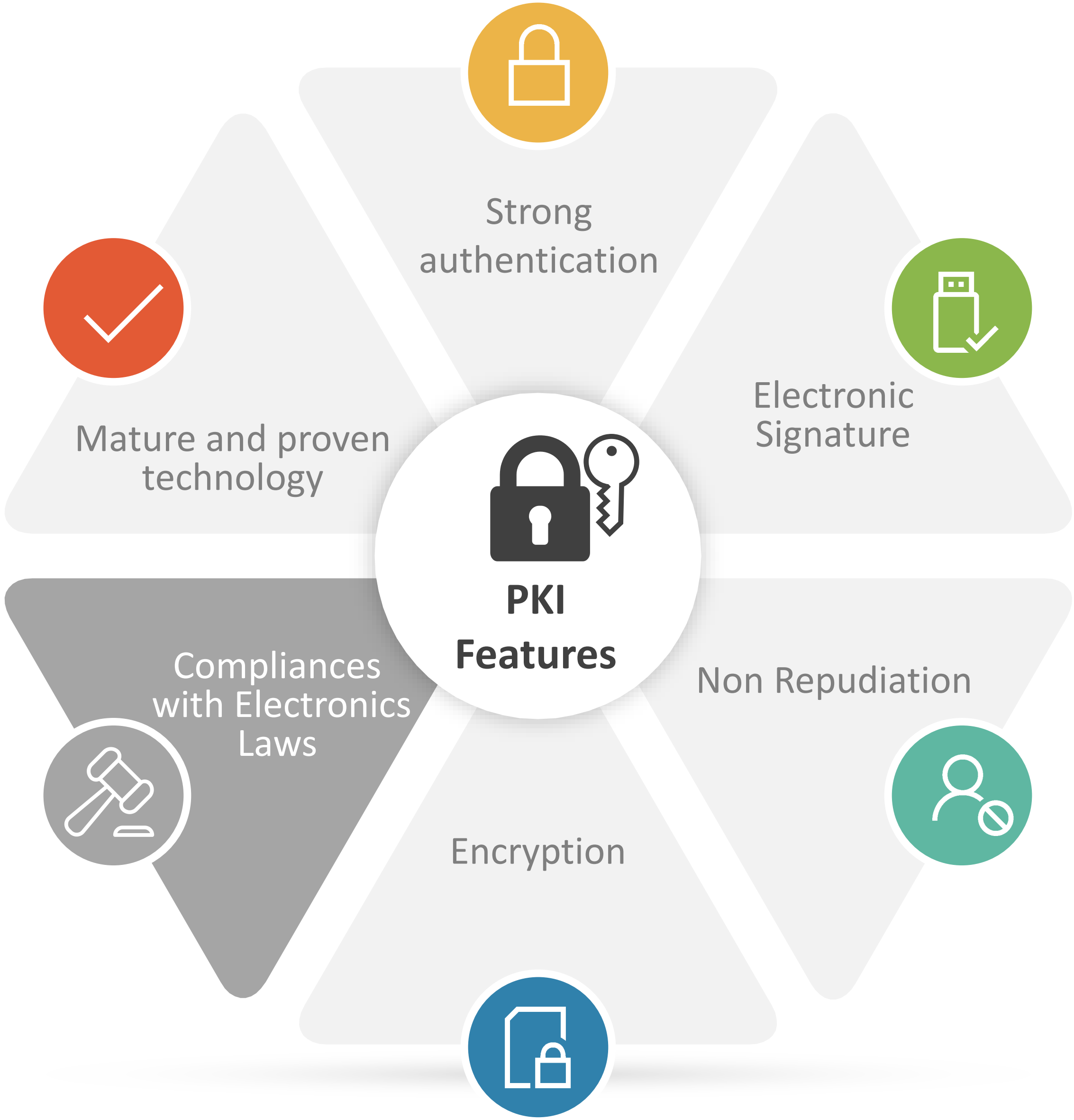
Non Repudiation

provides a reliable mechanism using PKI digital signature



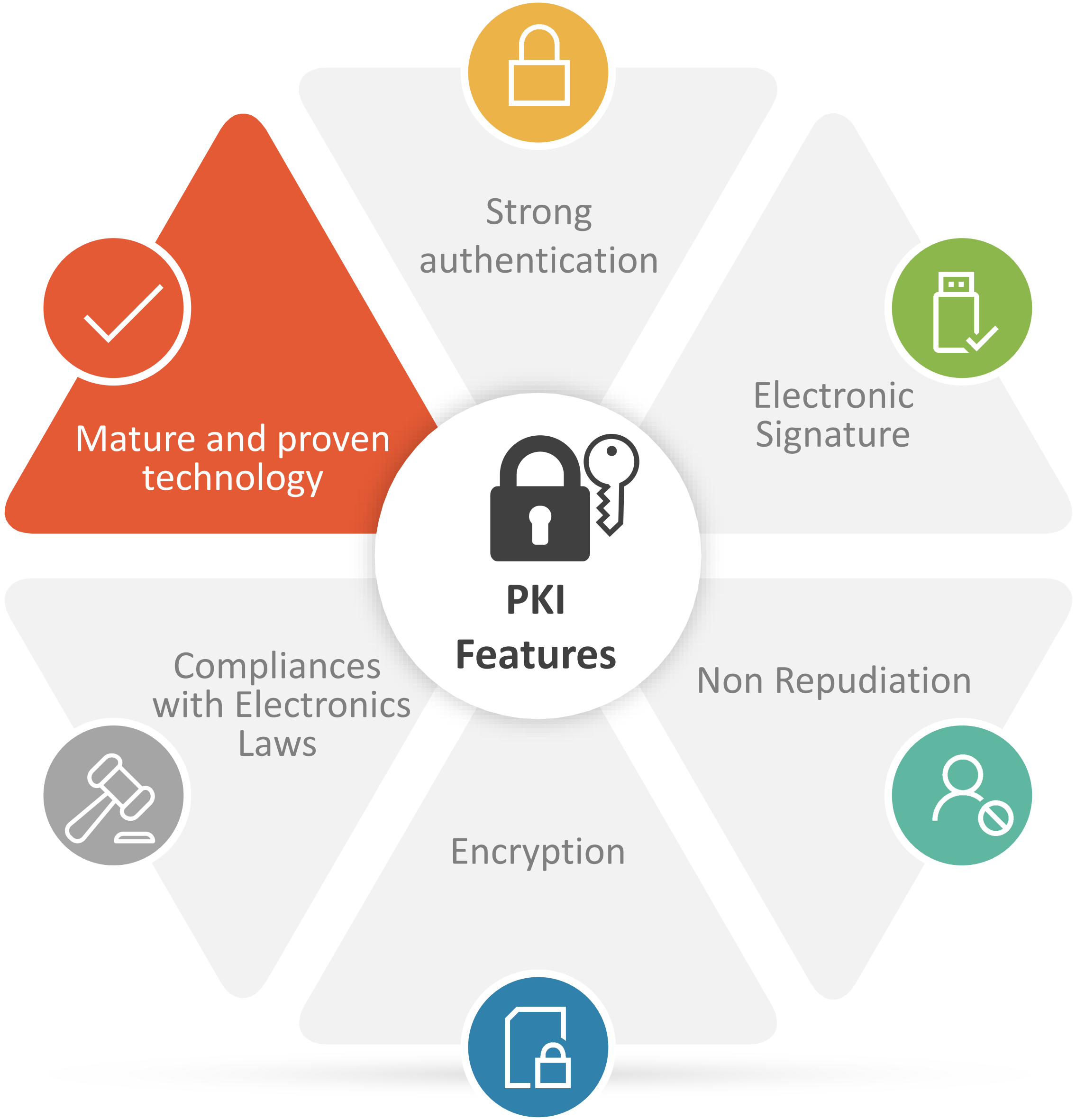
Encryption

to avoid unauthorized disclosure of data using public keys



Compliances with Electronics Laws

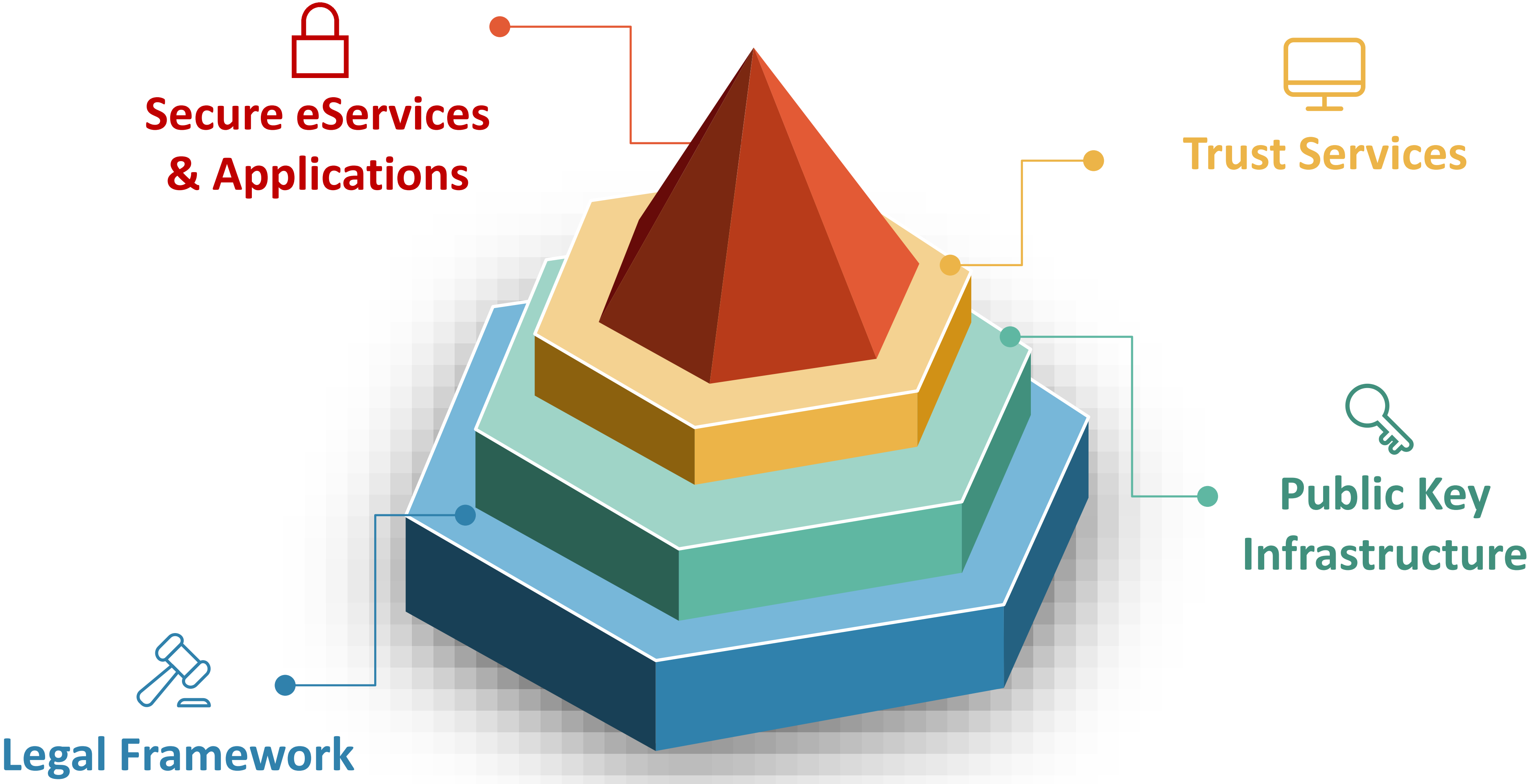
and regulations Leverage Data protection Acts and all around the world



Mature and proven technology

adopted for financial, governments, service providers offering highly and valuable services

eTrust Pyramid Components



eTrust Pyramid Components

Legal Framework

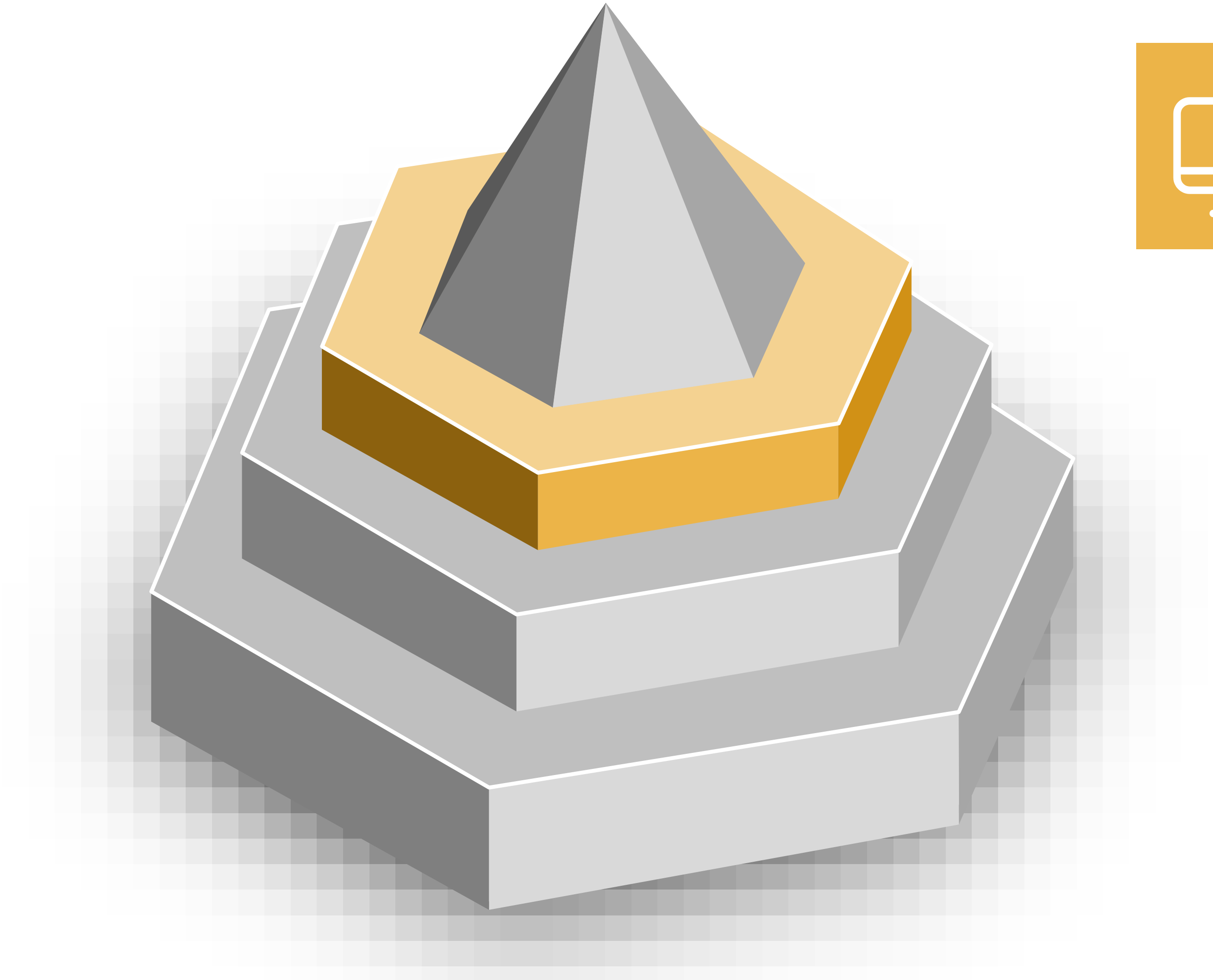
Oman E-transaction
Law/69-2008.

eTrust Pyramid Components

Public Key Infrastructure

- Policies, Procedures, People, Hardware and Software required for to generate, share and manage digital certificates.

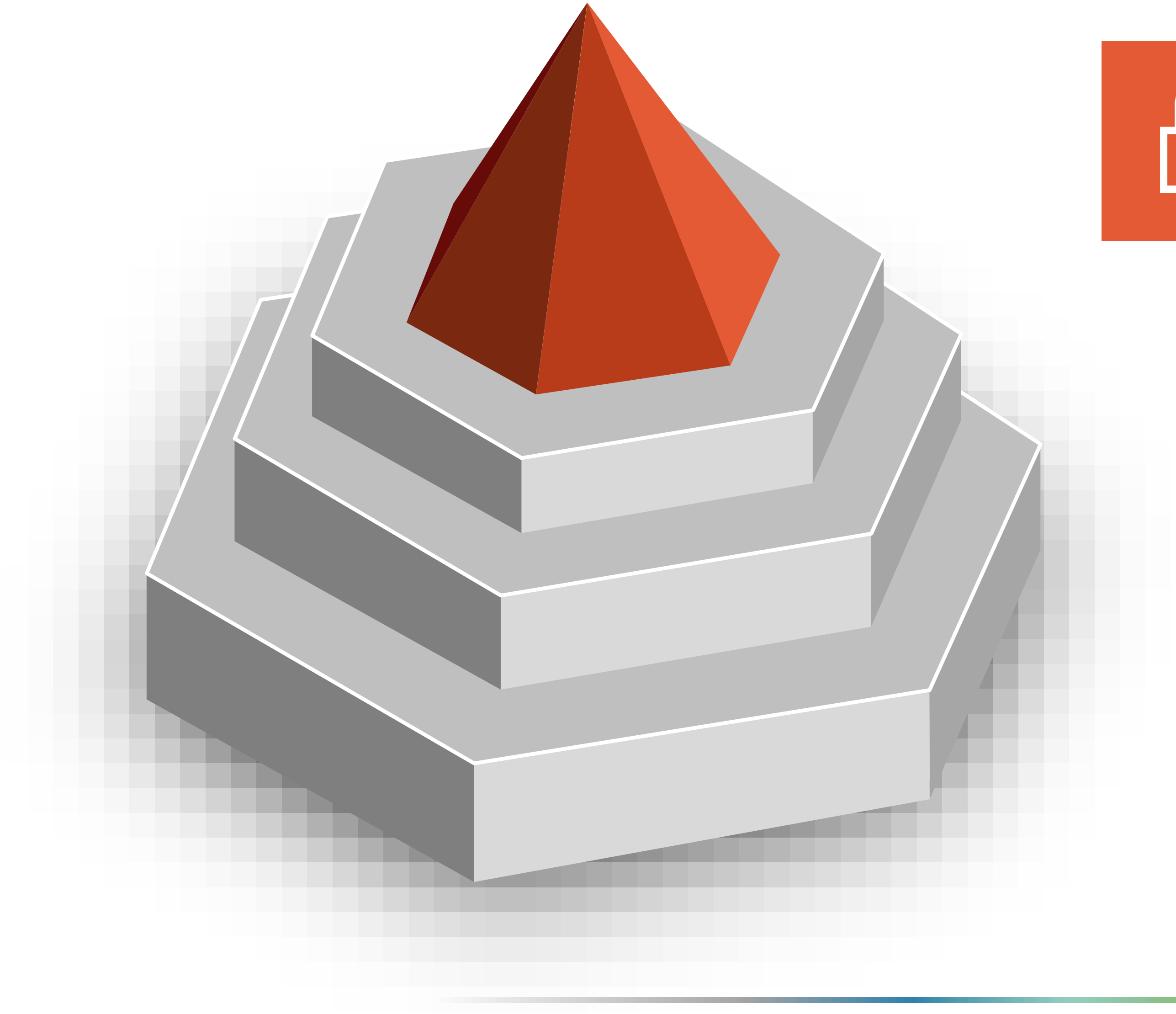
eTrust Pyramid Components



Trust Services

- Signature Validation Services
- Time Stamping
- On Line Revocation Services
- Publication of digital certificates and revocation list.

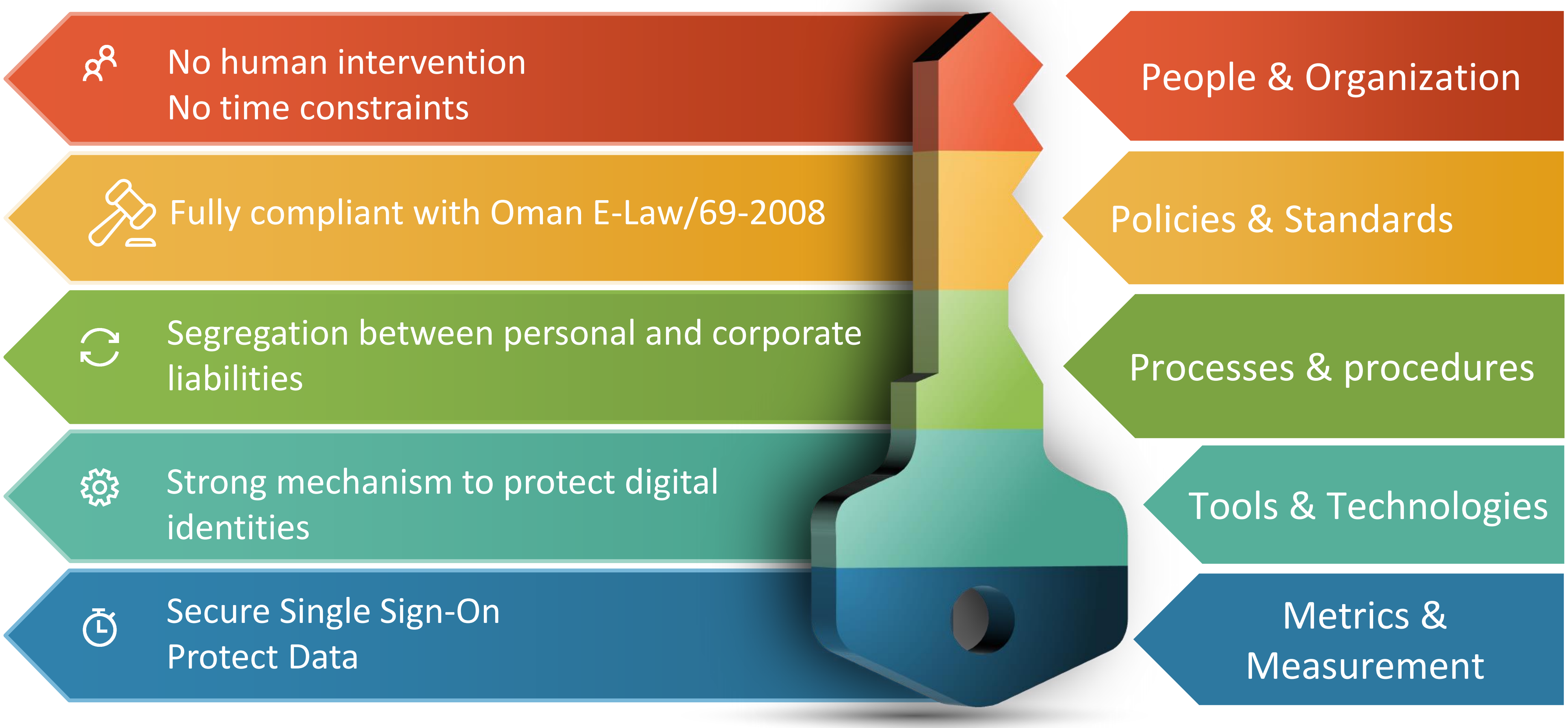
eTrust Pyramid Components



Secure eServices & Applications

E-Services require strong means of authentication, digital signing and data protection in accordance with the country laws and regulations.

ITA efforts for National PKI



No human intervention
No time constraints

Fully compliant with Oman E-Law/69-2008

Segregation between personal and corporate liabilities

Strong mechanism to protect digital identities

Secure Single Sign-On
Protect Data

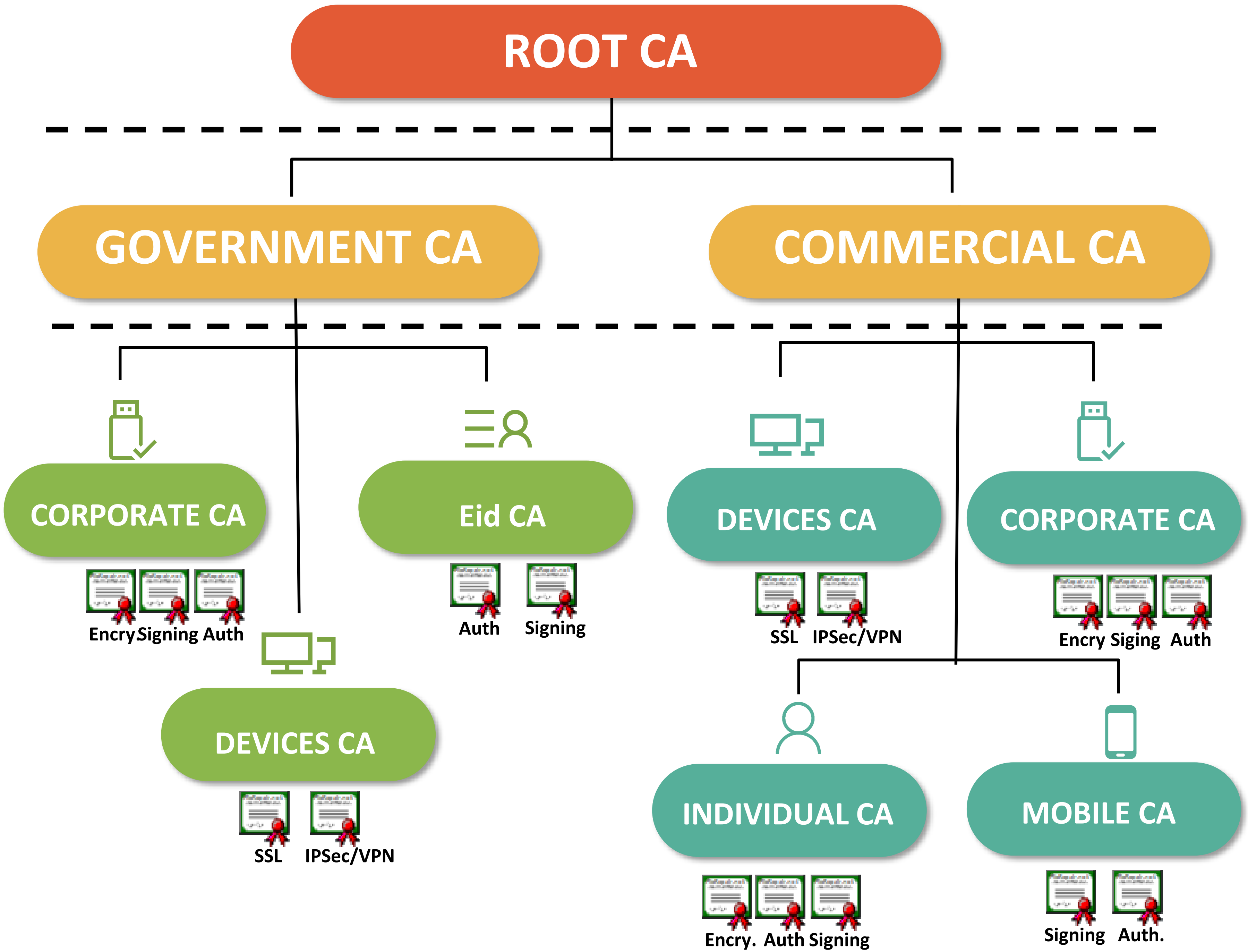
People & Organization

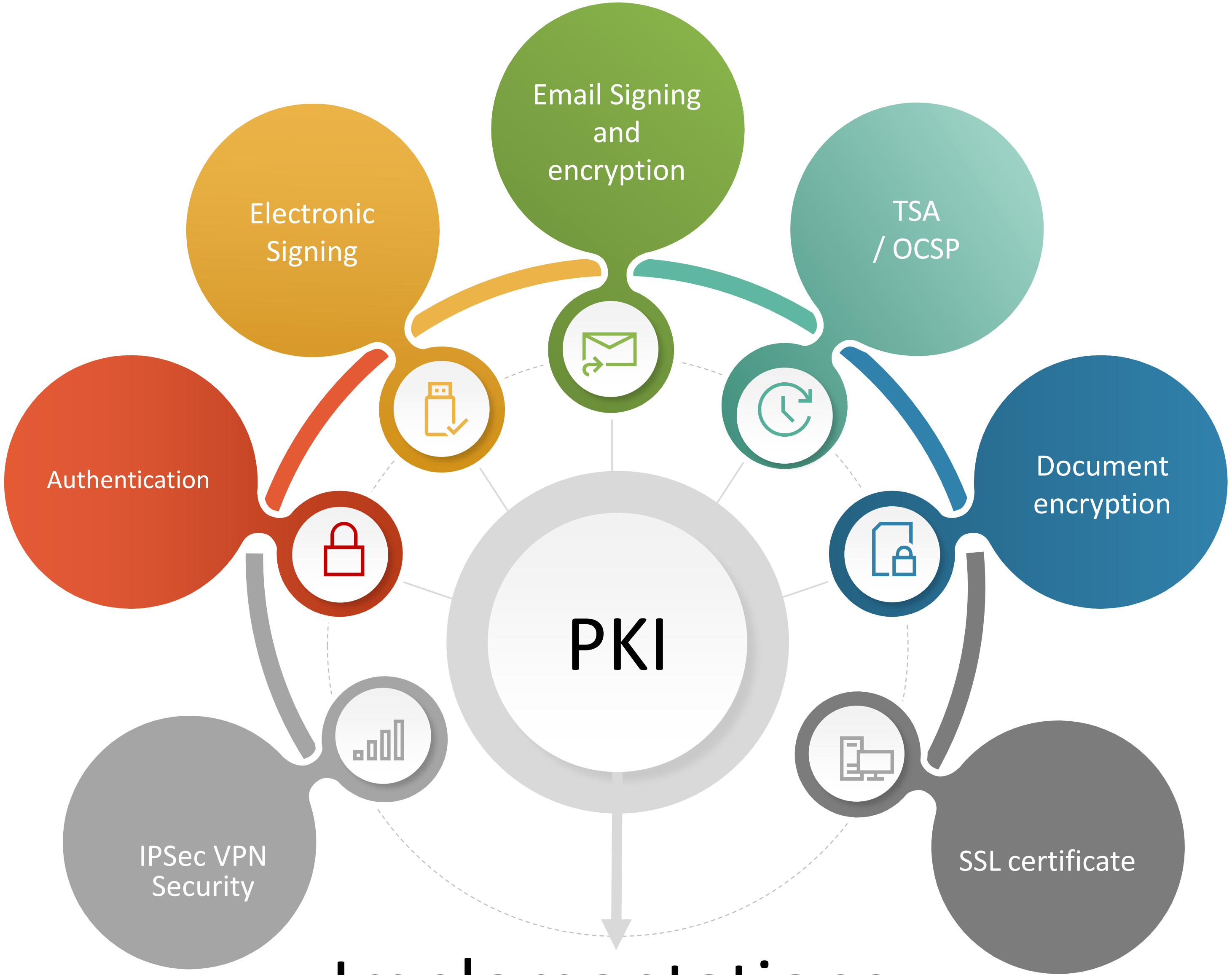
Policies & Standards

Processes & procedures

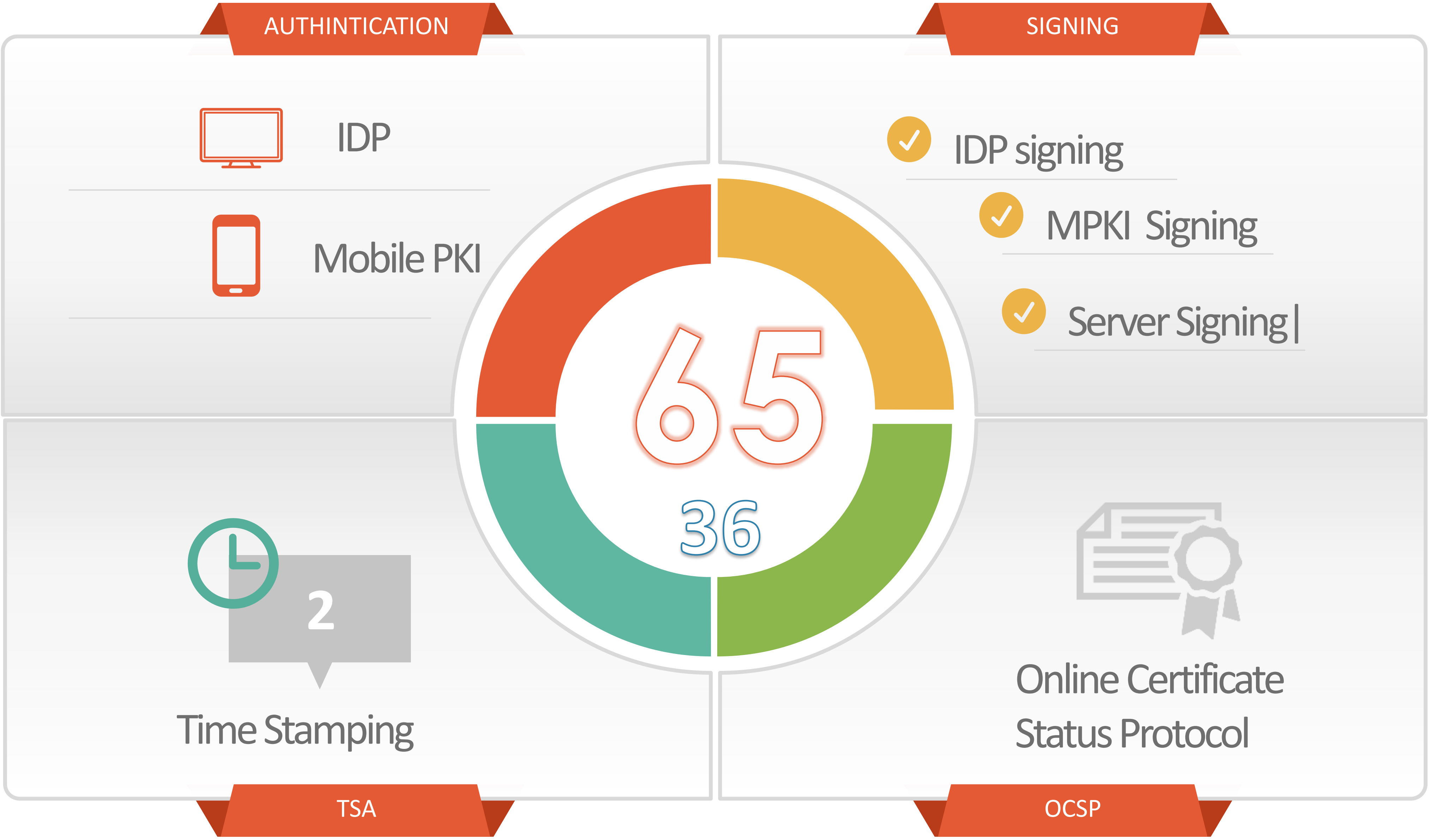
Tools & Technologies

Metrics & Measurement


ROOT CA
GOVERNMENT CA
COMMERCIAL CA
CORPORATE CA
Encry Signing Auth
Eid CA
Auth
Signing
DEVICES CA
SSL
IPSec/VPN
DEVICES CA
SSL
IPSec/VPN
CORPORATE CA
Encry Siging Auth
INDIVIDUAL CA
Encry. Auth Signing
MOBILE CA
Signing
Auth.



Implementations



AUTHINTICATION

IDP

Mobile PKI

SIGNING

✓ IDP signing

✓ MPKI Signing

✓ Server Signing|

Time Stamping

TSA

Online Certificate
Status Protocol

OCSP

Statistics

Integrations (1)

20 February 2019

- ROP NRS
- Omantel
- Ooredoo
- Invest Easy
- ROP Customs
- Ministry of Health
- Ministry of Manpower
- Rafd Fund

- ITA
- Muscat Municipality
- OPP
- MARA
- Mazad
- Bank Dhofar
- NCSI
- MRMWR

Statistics

Integrations (2)

20 February 2019

- Civil Pension
- MOI
- TRA
- PASI
- PACI
- SGT
- PAMR
- Oman Info
- Alduqum
- Oman Post
- PEIE
- ROP Traffic
- Central Bank
- MECA
- MAF
- MOJ

Statistics

Integrations (3)

20 February 2019

MCD

Tender Board

MOE

Oman Chamber

Statistics

Certificates

20 February 2019

National ID Card

AUTH SIGN

15.7 M

Mobile

AUTH SIGN

110,882

Statistics

Transactions

20 February 2019

National ID Card

14.2 M

Mobile

1.7 M

Statistics

Accreditations

20 February 2019

- Royal Oman Police
- Omantel
- Ooredoo
- Central Bank

External Registration Authority (RA)

Accreditation

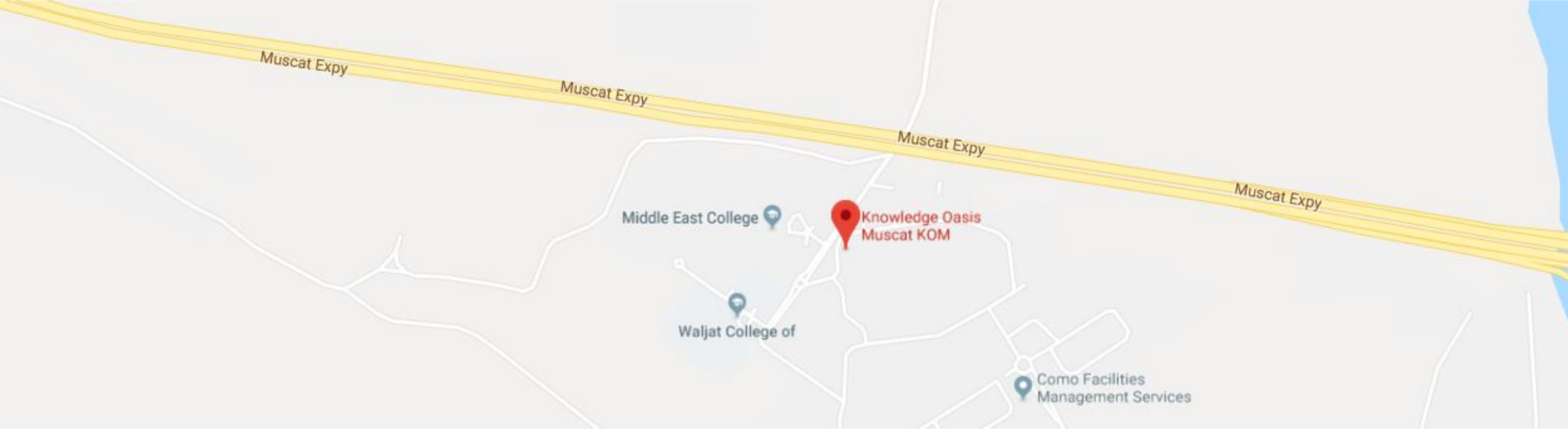
- An Entity can be accredited as an External RA to manage its own subscribers
- More convenient for conducting subscribers identifications
- Registration and Validation Teams will be trained by ITA
- Entity must be aligned with National PKI policies and accreditation agreement
- ITA will conduct auditing activities periodically and according to the auditing report, PMC might renew or suspend the accreditation

Sub-CA accreditation

Accreditation

- An Entity can be accredited as a Sub-CA and build its own technical solution
- Entity must request license according to the licensing processes
- Entity should meet all the policies and the accreditation agreements approved by ITA
- ITA will conduct auditing activities periodically and according to the auditing report, PMC might renew or suspend the accreditation

THANK YOU



ADDRESS

Information Technology Authority (ITA)
is based in Knowledge Oasis Muscat
(KOM) building 3, Second Floor.
☎ | (+968) 24166440
📅 | 7:30 to 14:30

EMAIL

ndccservices@ita.gov.om

SOCIAL MEDIA

eoman_ita

eOman

eoman_ita

eoman.ita