THALES

Establishing identity and maintaining privacy in the cloud

The need for Hardware Security Modules

Jonathan Allin

EEMA 4-5 July 2017

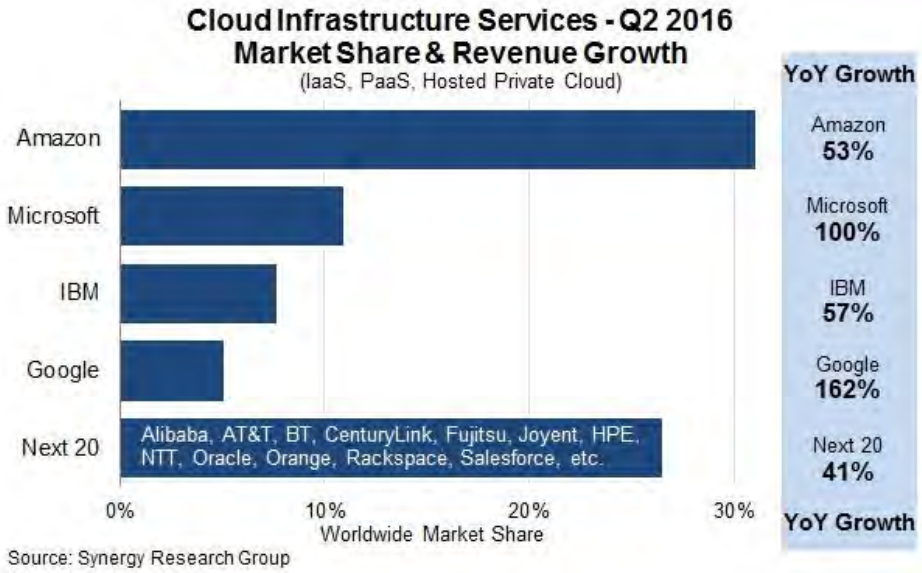
What we'll talk about

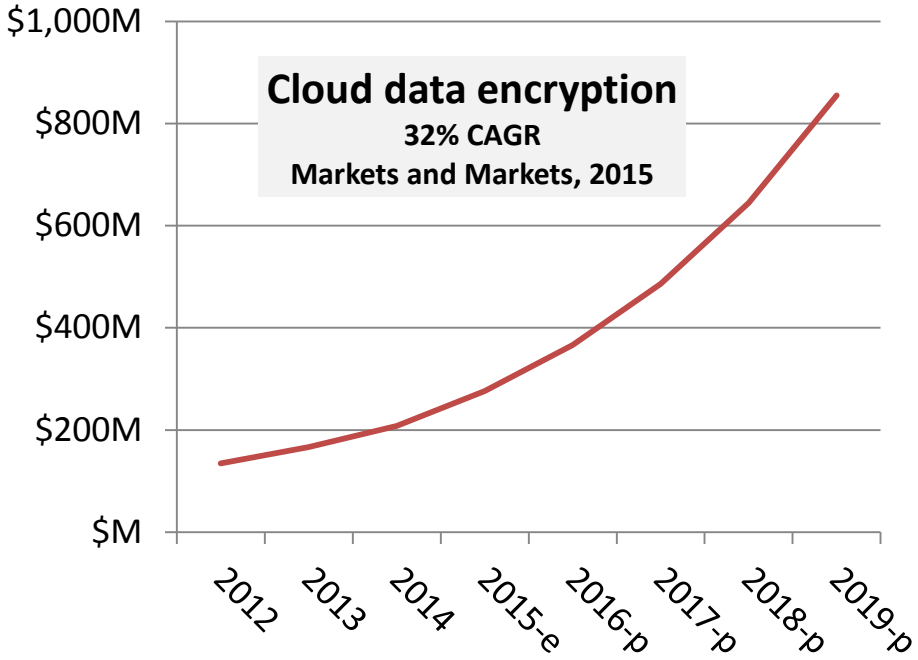
- The cloud: its growth, its ubiquity, how we use it
- When HSMs are required (or at least highly desirable)
- How an HSM fits in: a couple of examples

Growth in the cloud

- By 2020, at least 35% of new IT spending in Europe will be cloud-based
  - while non-cloud enterprise applications spend will be flat

IDC, 2017





- More than 70% of European enterprise IT organizations will commit to multicloud architectures in 2018

IDC, 2017

We transact in the cloud

Gov⇔Citizen

Business⇔Business

Business⇔Customer

Me ⇔You
??

Business⇔Business

Consumer⇔Retailer

We trust the cloud with sensitive information

Office 365

salesforce

snapfish

OPEN

THALES

Why use a Hardware Security Module

Regulatory compliance

Internal audit requirements

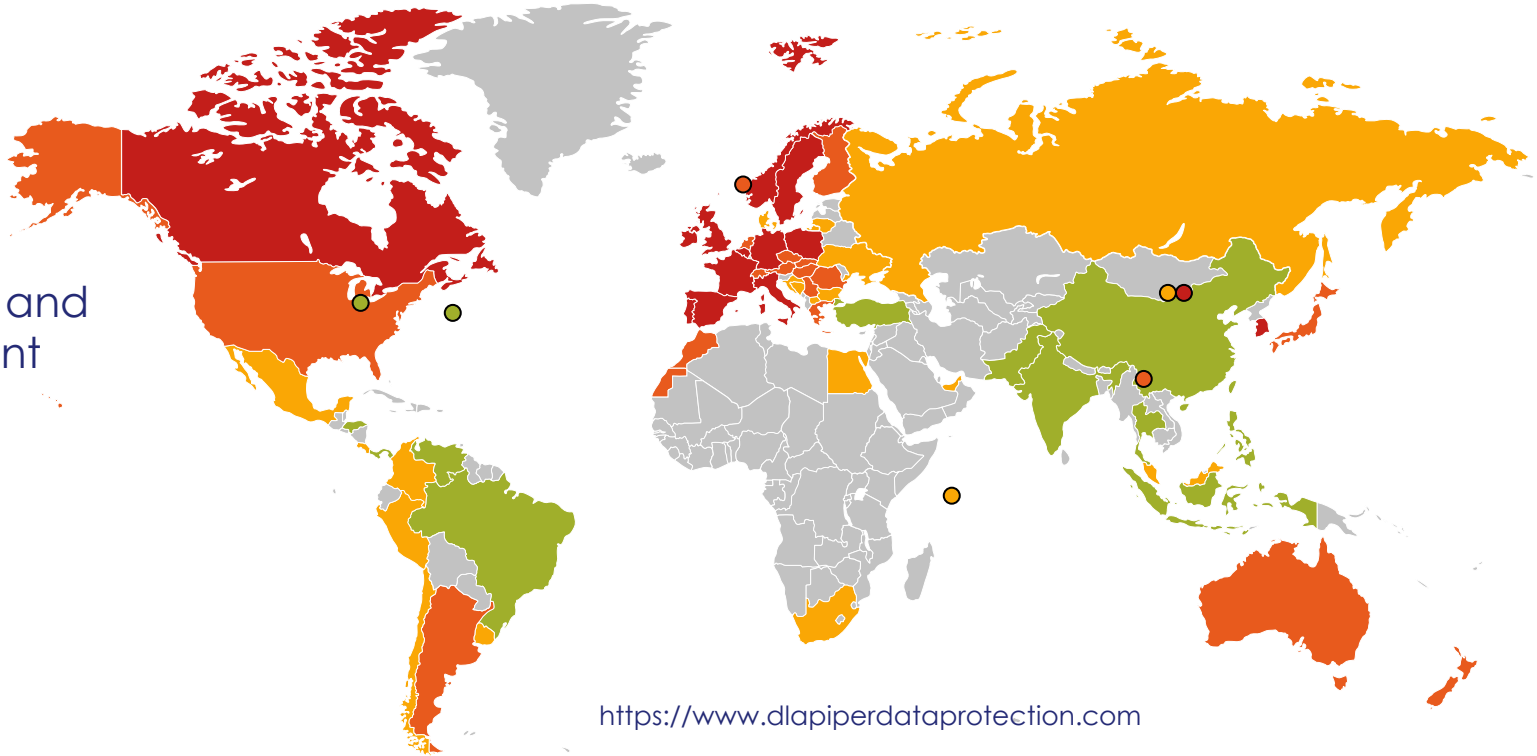
Protect valuable assets in a high threat environment

Fear: one data breach too many

Regulatory compliance can require HSMs

GDPR PSD2 eIDAS

- Regulation and enforcement
  - **Heavy**
  - **Robust**
  - **Moderate**
  - **Limited**



https://www.dlapiperdataprotection.com

Some of the regulations

PSD2 "regulatory technical standard" article 34

- "For the purpose of identification ... payment service providers shall rely on **qualified certificates** for **electronic seals** as referred to in Article 3(30) of [the eIDAS Regulation,] or for **website authentication** as referred to in Article 3(39) of that Regulation"
- Qualified certificates ⇨ eIDAS compliant HSMs

GDPR

- Applies to any multinational company that
  - collects and retains customer data, trade secrets, and other confidential data
  - or operates in a critical infrastructure sector, such as energy, financial services, healthcare, and defence
- Right to be forgotten ⇨ HSM for key life cycle management
- Show best practice ⇨ data encryption, logging and audit trails ⇨ HSM

SAFE-BioPharma

- Created by the biopharmaceutical industry and its regulators to provide trust for digital transactions in biopharmaceuticals and healthcare
- Common standards for Id and PKI ⇨ HSM for key protection and secure signing

What are Hardware Security Modules?

Tamper resistant cryptographic devices

- Isolated from threats that can come from the host OS, or from applications running on the host

What should an HSM do?

- Protect cryptographic keys from theft and abuse
- Simplify key management
  - replication, recovery
- Control how a key can be used
- Securely execute cryptographic operations
  - encrypt, sign, time stamp, authenticate, …
- Ensure or help compliance with industry regulations
- And so as far as possible to delegate our trust to the HSM

Where are Hardware Security Modules being used?

Identity trust infrastructures

- Natural person
- An organisation
- eIDAS provides a general source of identity
  - For both natural persons and for organisations

Signing

- Document, transaction, application code
- Who signed, what was signed, when it was signed

Protecting stored data

- Only allow authorised access

Protecting transmitted data

- Only allow authorised readers
- Detect tampering

Identity and authentication

Two separate questions

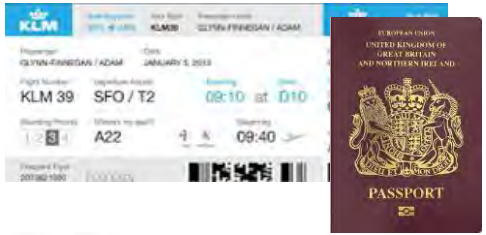
- Who am I - authentication
- What am I allowed to do - authorisation

Appropriate strength of identification

- May need to identify the natural person
- Or name and password may be sufficient
- Or simply possession of a transferable token or ticket

Examples

[●●●●]



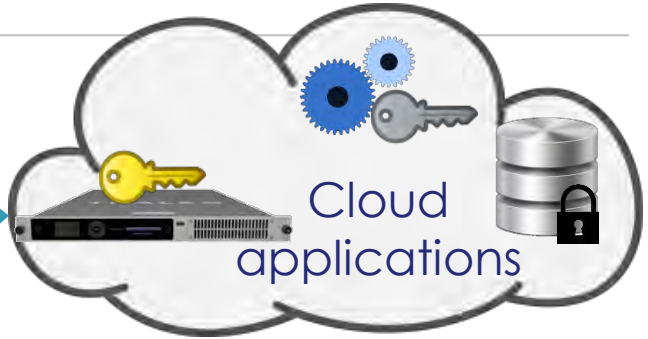
p.body
[●●●●]

OPEN

THALES

Protecting data in the cloud

Key is secured by an HSM in the cloud, HSM protects customer's logs



Key is available for use by security sensitive cloud applications, and to access the customer's encrypted data
Cloud provider has no access

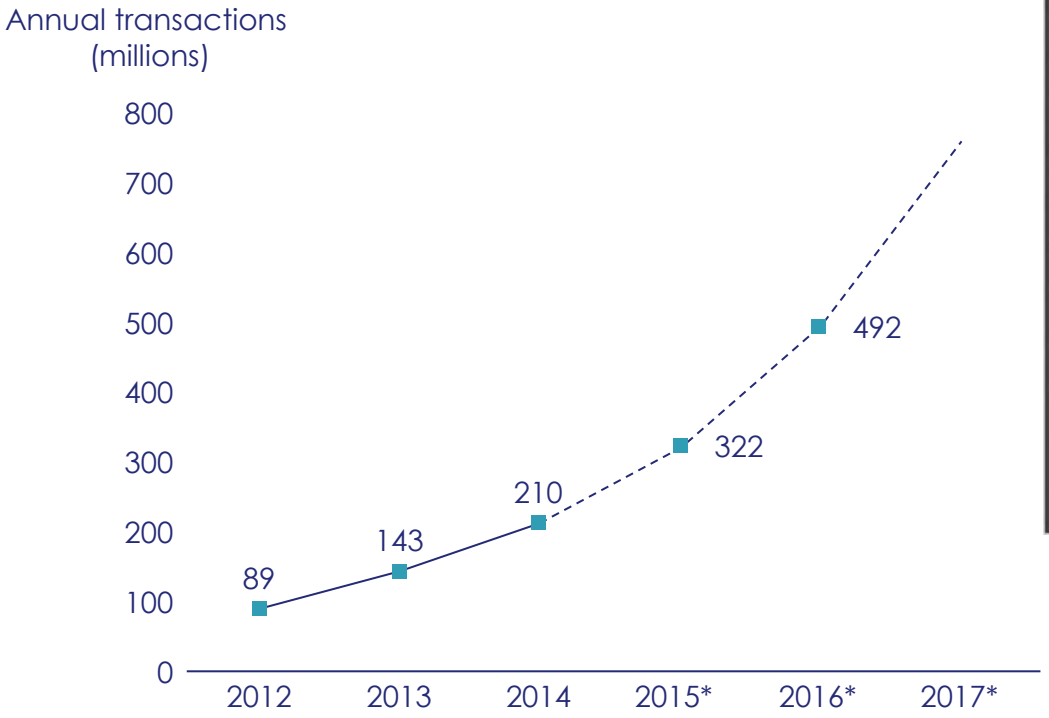
HSM wraps and exports the key to the cloud

Customer's premises

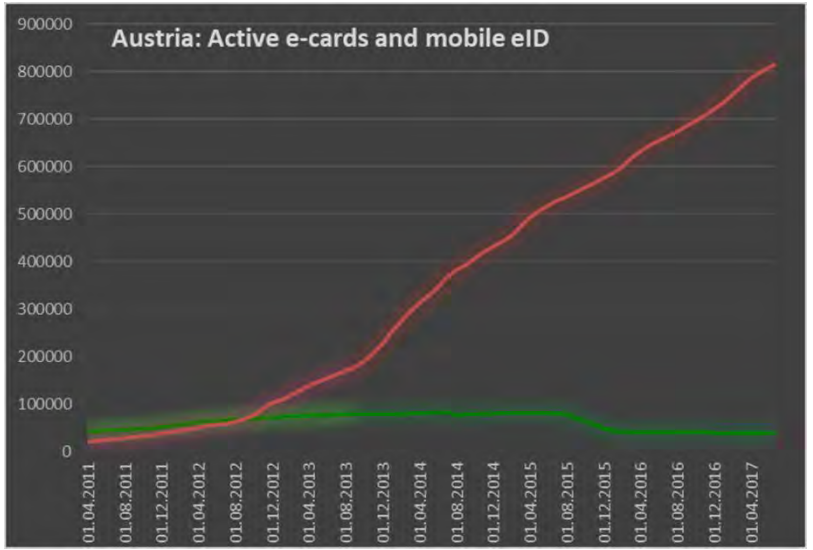
Customer uses an HSM on their premises to generate their key(s)
HSM provides secure long term storage and disaster recovery for those keys

THALES

Increasing adoption of electronic signatures



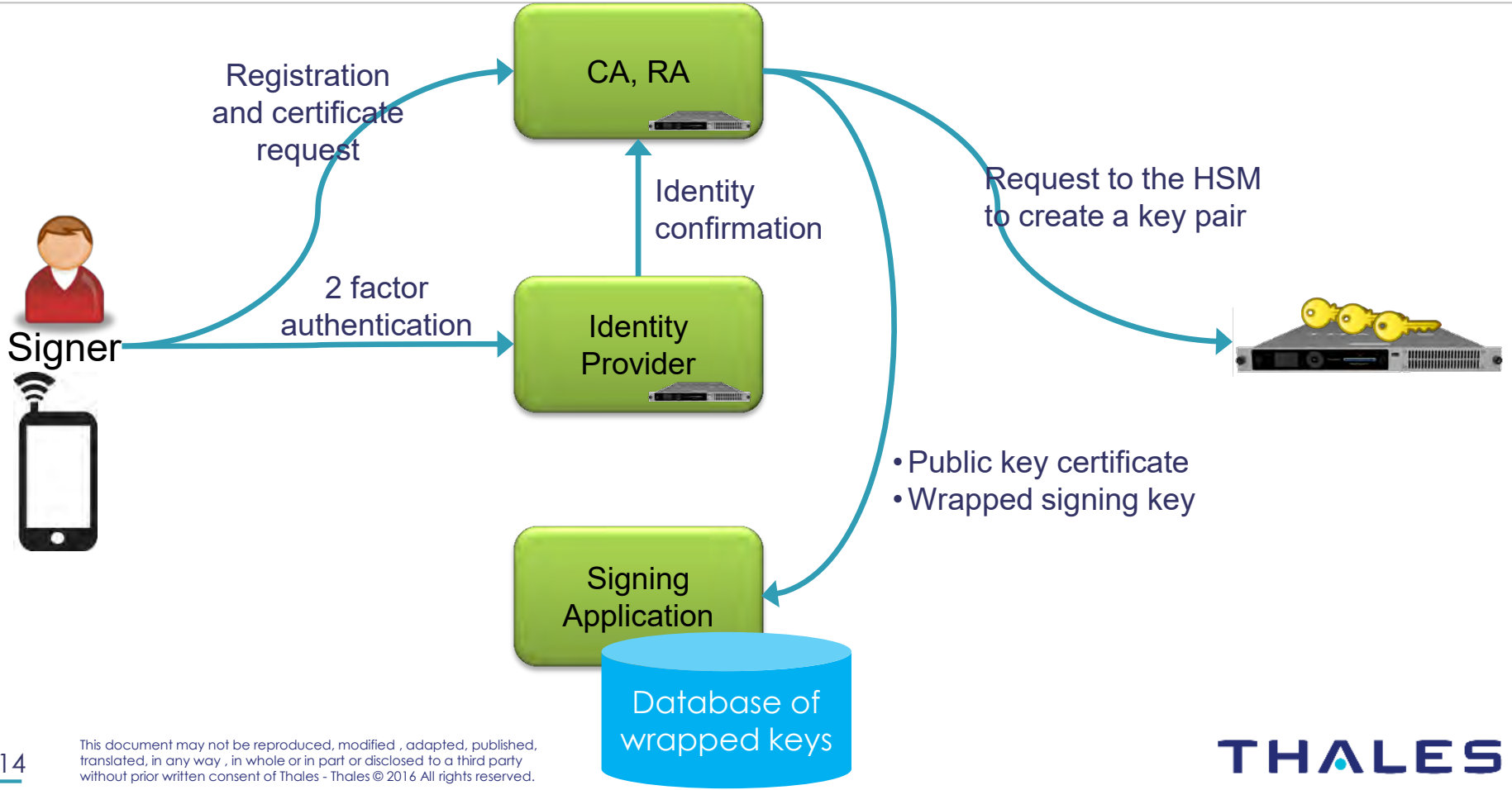
Source: Forrester interviews with 9 leading eSignature solution providers
* Forrester projection



-Smart cards- -Mobile eID-

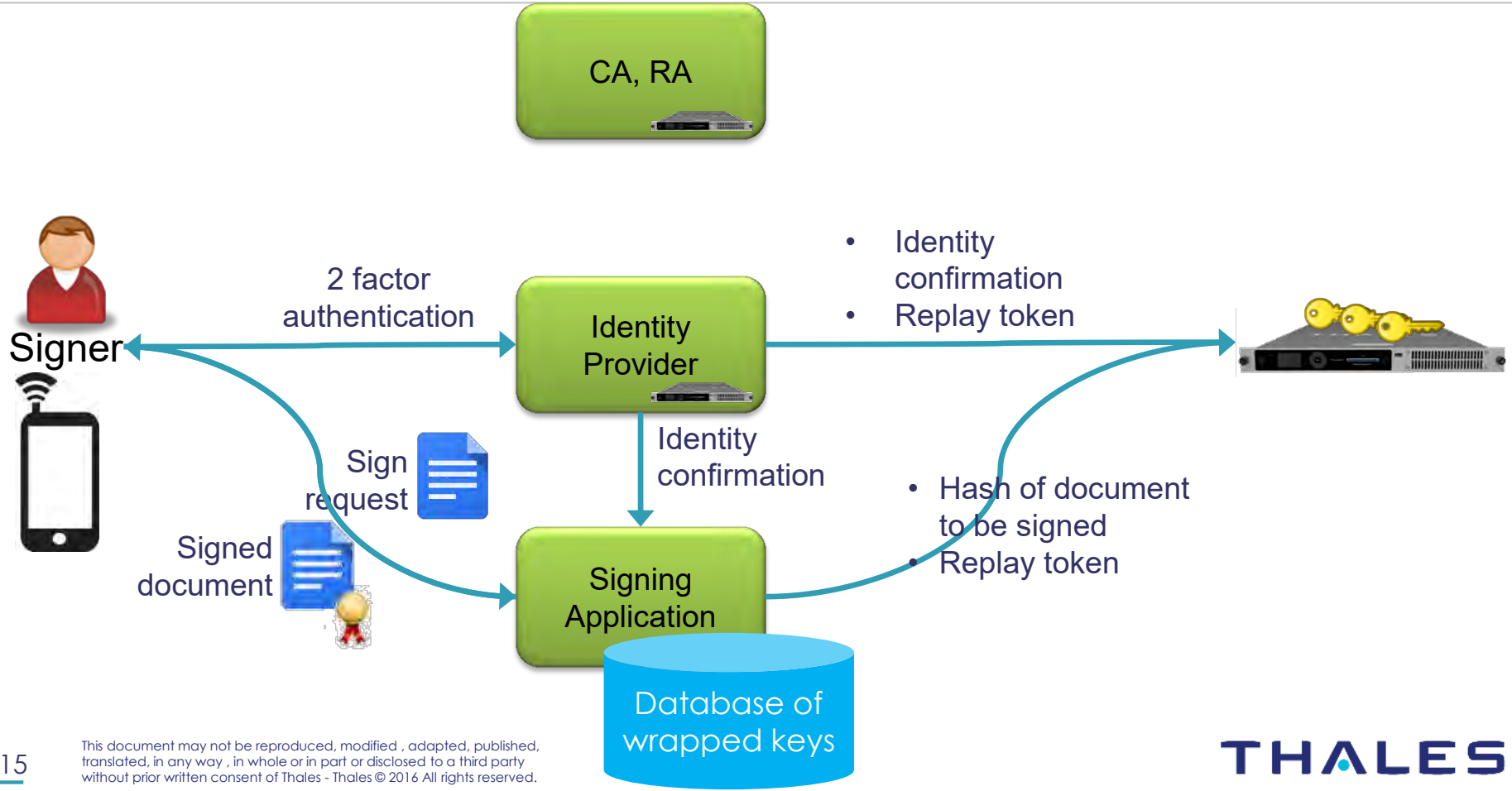
- Austria, Italy, Spain, Sweden
- India, Japan

eIDAS compliant remote signing architecture: registration



THALES

eIDAS compliant remote signing architecture: signing



THALES

We have a responsibility to …

Protect our own identity and our personal data

Do what we can to protect the identity and personal data of others


ANY
questions?