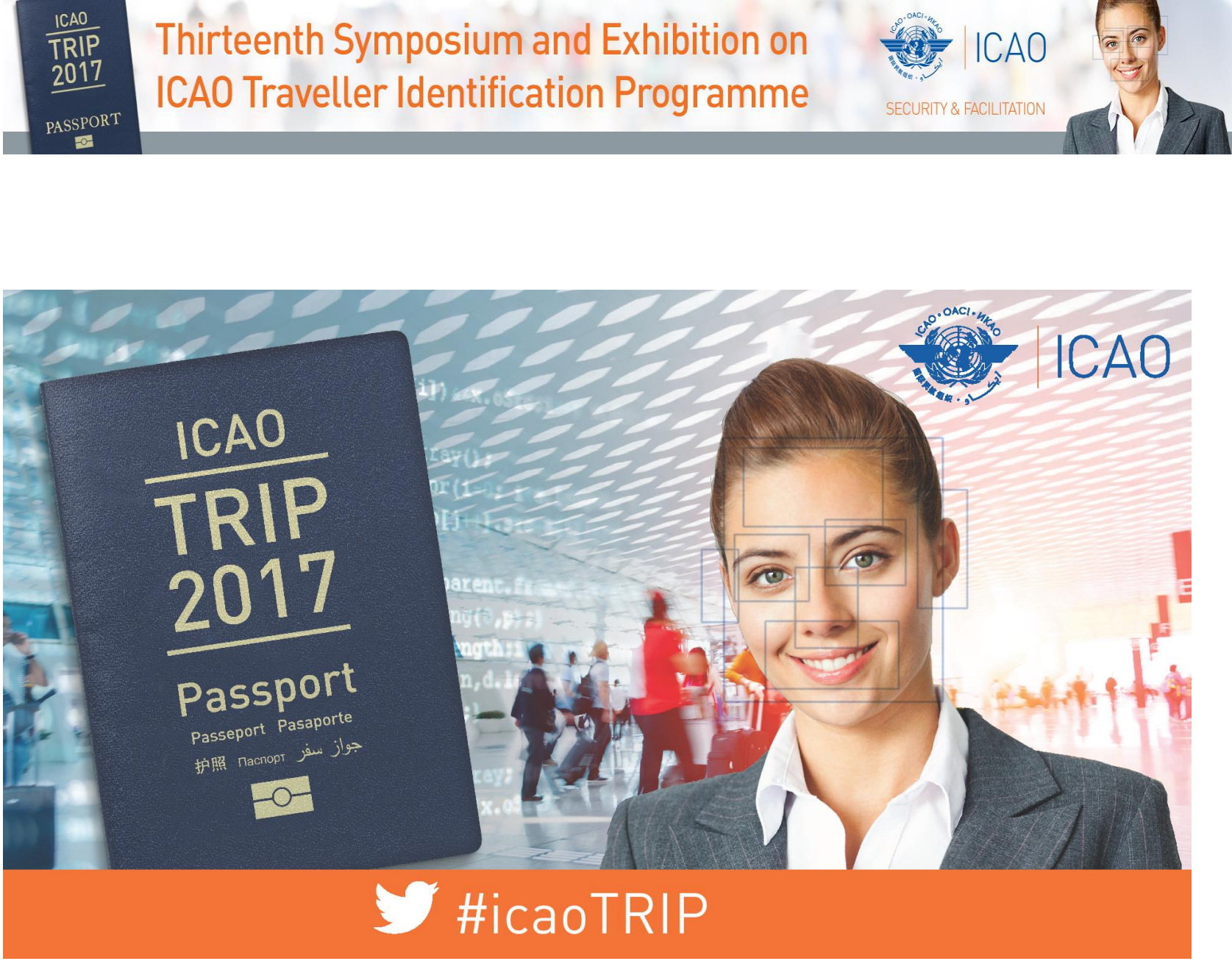

ICAO
TRIP
2017
PASSPORT
Thirteenth Symposium and Exhibition on
ICAO Traveller Identification Programme
ICAO
SECURITY & FACILITATION
ICAO
TRIP
2017
Passport
Passeport Pasaporte
护照 Паспорт جواز سفر
ICAO
#icaoTRIP

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Justice and Police
Federal Office of Police, fedpol

PKI/PKD Requirements, Challenges & Opportunities

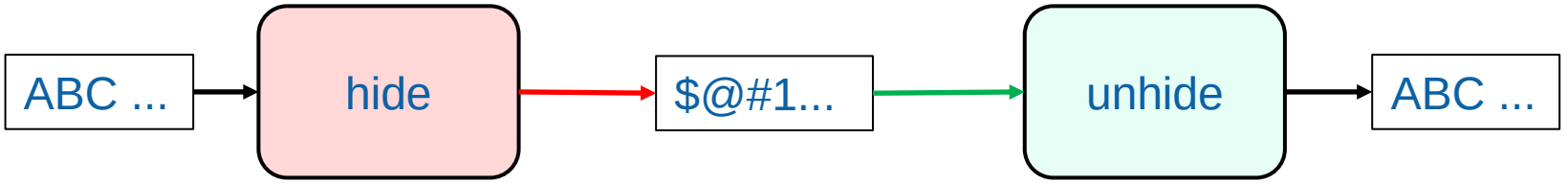
Arnaldo Cremisini
Senior PKI Officer
Federal Office of Police fedpol
Switzerland

ICAO PKD Workshop
Montreal, 23 October 2017

Public Key Infrastructure … destroying the myth

As soon as we are confronted with PKI, we hear some possibly "frightening" words such as Cryptography, Key, Hash, Signature … let us try to discover what they are and find a common "jargon"

Cryptography is simply the "art" of hiding and un-hiding information



This is achieved through some kind of mathematical process using objects called Keys

Mathematicians tell us that there are couples of **objects** tied together (**keys**) which are able to hide and correctly uncover the information

If you keep **Key 1 (PRIVATE) secret** and **well protected** … this means that all people knowing your **Key 2 (PUBLIC)** are able to "uncover" your protected information and at the same time, they know it comes from you and only from you!

The PKI (Public Key Infrastructure) is "the entity" in charge of the definition, use and protection of the keys.

As soon as we talk about keys, secret … publication etc. we understand that many things might be involved such as roles, people, organisation, policies, financial aspects, infrastructure etc.

But PKI is all about mathematics and objects (keys), isn't it?

… well, not really…

The experience shows that keys and mathematics involves less then 5% of a PKI and more then 95% is about organisation, policies, roles, infrastructure etc. … which in turn is about responsibility and management.

Now the question that arises is: Are there any rules to identify the organisation in charge of and operating such a PKI?

… I'm afraid I have to say NO.

It depends on your country and organisation, who should be put in charge and how
… **there is no recipe**
The Swiss case just as an example:

The first organisation confronted with the issuance of eMRTDs was the Federal Office of Police and, at that time, the decision was taken for the sake of simplicity, that the same office should also be defined as responsible for the Swiss PKI.

This was stated in the law so that also the legal conditions were met to allow the Federal Office of Police to create the Swiss eDoc PKI.

The eMRTD's issuer perspective …

After you have identified the organisation that will take care of your PKI, ICAO helps you with the Doc 9303 and allows you to identify the relevant aspects (technical and to some extent organisational).

You then, have to consider to create and operate your PKI and further on, to issue your own eMRTDs …

… and with the help of cryptography and your keys, you also make sure that the data stored onto them truly comes from your country.

At an international level, ICAO defines such a PKI organisation as your **national** and **unique** **CSCA** (Country Signing Certification Authority) …

… yes, it is a Certification Authority, because it certifies that the data stored in the documents - protected by its Private Key - are authentic.

Now we have an organisation (PKI), a name for it (CSCA), the keys … and we can issue authentic and secured eMRTDs …

But what about the verification of such an authentic eMRTD?

The eMRTD's world as seen by the verifier …

We have seen that the knowledge of a public key allows verifying the content of an eMRTD document … but we have to make sure that the public key is authentic and really, really comes from the document's issuer.

Well, all this is about … Trust …

Just exchanging "hidden" (encrypted) public objects is not really practical … therefore the public keys are embedded into a further structure - that to some extent - declares which are the properties of your PKI and what - you allow - the keys to be used for.

These objects are called Certificates and they must underlie the requirements specified in the ICAO document Doc 9303 … and they are authentic, because you provide the proof through your secret and well protected private key.

Now, assuming you are able to retrieve somewhere the Swiss certificate …

… how can you be certain that this certificate really comes from Switzerland …

… and if you can prove that this certificate comes from Switzerland …

… but if it does not comply with the rules and requirements of ICAO …

… what kind of trust can you apply to this object … and finally to the eMRTD it certifies?

The Public Key Directory

The verifier has first to retrieve (find, acquire etc.) the issuer's CSCA certificate and then prove it is authentic …

The past experience has shown that finding an eMRTD's CSCA certificate was (is) not an easy mission.

Doc 9303 6th edition required the CSCA certificates to be exchanged by diplomatic channels; this was – to some extent – a quite difficult task and not always successful.

New in the 7th edition of the same document, is the requirement to acquire – by several and different channels - the certificate and verify it through "out-of-band" means.

Now the time comes, to consider an important missing piece of our "puzzle" …

the PKD (Public Key Directory)

In an "ordinary" PKI, the PKD is used to "publish" the certified public objects (e.g. certificates) belonging to the same PKI …

... in the eMTRD's world the PKD has a much broader goal …

It is used to collect national as well as international certificates, verify their authenticity and finally provide them to the border control to allow this organisation to verify the digital content of the eMRTDs.

The Public Key Directory … the mission

As we previously said, everything at PKD level is about trust …

This is important when you have to prove the authenticity of the public object, such as certificates.

The "out-of-band" verification plays an important role, but it also has to rely on a well established relationship between the issuer and the verifier …

… what "out-of-band" might mean …

Assume, that (now) you know who I am; and you trust (for some well founded reasons), that I come from Switzerland and represent the Swiss PKI …

… if I would give you the Swiss (public) certificate and confirm to you it's authenticity; could you believe me and "recognise" it as authentic?

I suggest, you should not ! …

A trivial interpretation of "out-of-band" may suggest that you verify the authenticity through, at least, another "channel" …
… as an example you may contact another Swiss Federal Office (that you know you can rely upon) … and ask them to confirm the certificate I gave you …

… but first of all, you always have to get your hands on that certificate …

… no end to the concerns?

You got the certificate … and it is authentic … proved by several independent means …

… but what about the issuer's PKI? …

…and what about the certificate compliance toward the requirements …

To enhance the trust the issuer should tell the verifier a bit more about its PKI …

The best way to increase confidence, is to anchor in a document how you handle your PKI; just write down the policy related to your organisation, your infrastructure … so that everybody having access to your public objects (such as certificates, eMRTDs etc.), feels comfortable in using them …

… but "errare humanum est" ... (Latin: making mistakes is part of being human)

… and certificates (just to recall: they are used to publish your public keys), do not always conform to the specifications …

… now, if the non-compliance is serious, it might provoke some – major - issues at the verifier site … e.g. it might cause some problems at the border, not allowing the verifier to rely on your eMRTDs … but even minor certificate's issues might cause serious problems …

… and what happens with our citizens traveling around the world?

The last EU Interoperability tests, held in Italy in September 2017, showed that only 17 out of 40 certificates were compliant …

… in an "ideal new world" …

… there is always a solution …

the issuer has to produce the keys … the certificates … and verify the compliance …
… and publish them … and …

the verifier must find and retrieve the certificate … check their compliance with the specifications … and verify the authenticity …

Assume that in this world all countries would be **member** of the **ICAO PKD** …
(great!)

…we could verify the compliance of our certificates and further public objects even before issuing and/or publishing them

…we could publish our own certificates through authentic lists (called Master Lists)

…we could even publish - in these lists - the certificates we acknowledged and proved to be authentic …

We would make the mission of the issuer and of the verifier …
… much easier, more reliable …

… and eventually enhance the overall confidence in the eMRTDs and border security …

Any questions ?

Thank you

Contact details

Name: Arnaldo Cremisini
Email: arnaldo.cremisini@fedpol.admin.ch