Applicability of ABC4Trust in ITS

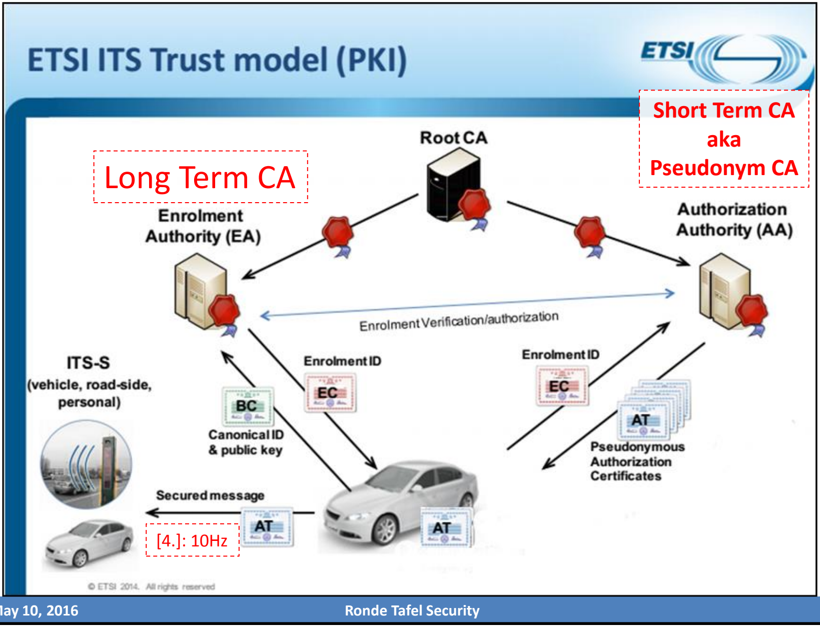
a quick scan inventory

Eric.Verheul@keycontrols.nl

Agenda

- ITS infrastructure
- Scope of quick scan / methods used
- Identified requirements
- Current ITS setup based on Crude PKI
- Comparison Crude PKI with requirements
- Issue first, activate later (IFAL) principle
- ABC4Trust techniques in ITS
- Comparison ABC PKI with requirements
- Progress in ABC PKI techniques
- Conclusion
- [Appendix: references]

ITS infrastructure context (from [1.])



ETSI ITS Trust model (PKI)

Long Term CA

Short Term CA aka Pseudonym CA

Root CA

Enrolment Authority (EA)

Authorization Authority (AA)

Enrolment Verification/authorization

ITS-S (vehicle, road-side, personal)

Enrolment ID

Enrolment ID

Canonical ID & public key

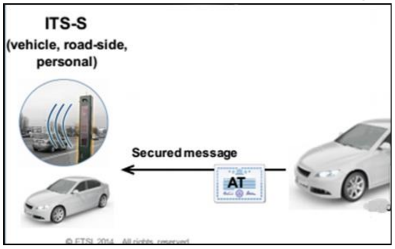
Pseudonymous Authorization Certificates

Secured message

[4.]: 10Hz

© ETSI 2014. All rights reserved

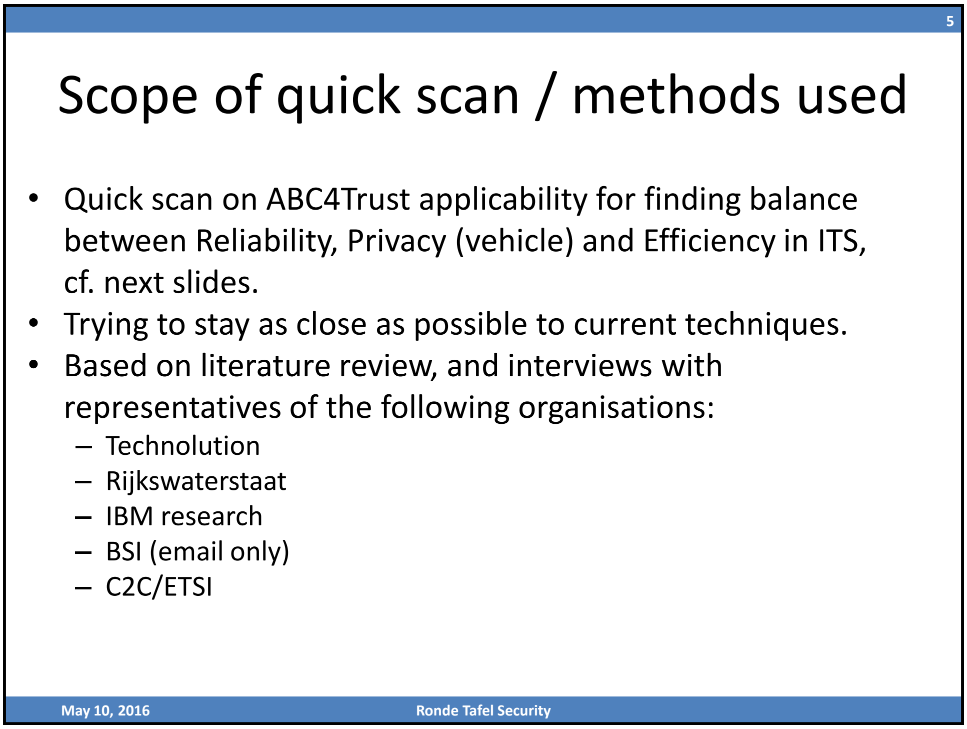
ITS infrastructure context (from [1.])



ITS-S (vehicle, road-side, personal)

Secured message

- Cooperative Awareness Basic Service (CAM) messages [8.] sent by vehicles are most relevant. These relate to e.g. vehicle position, speed and acceleration.
- *Receiving Parties* are other vehicles and roadside equipment.
- Decentralized Environmental Notification Basic Service (DENM) [9.] are not very relevant as they originate from roadside equipment.
- Emergency vehicles with special CAM attributes “lightBarSirenInUse”, “emergencyPriority” are out of scope of our inventory.

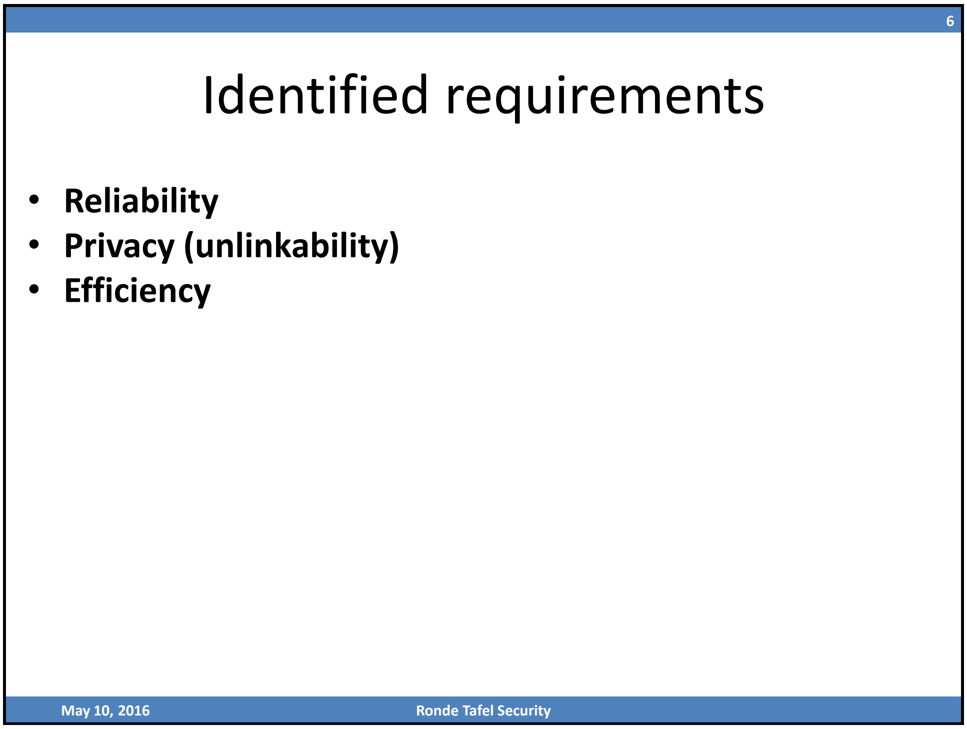


5

Scope of quick scan / methods used

- Quick scan on ABC4Trust applicability for finding balance between Reliability, Privacy (vehicle) and Efficiency in ITS, cf. next slides.
- Trying to stay as close as possible to current techniques.
- Based on literature review, and interviews with representatives of the following organisations:
  – Technolution
  – Rijkswaterstaat
  – IBM research
  – BSI (email only)
  – C2C/ETSI

May 10, 2016 Ronde Tafel Security

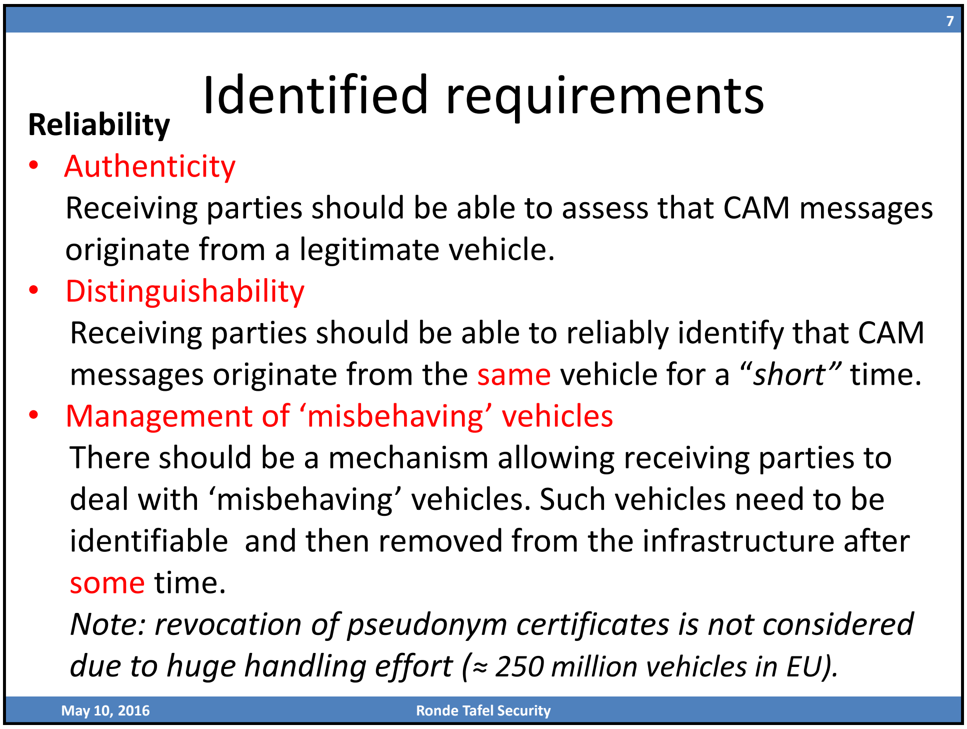


6

Identified requirements

- **Reliability**
- **Privacy (unlinkability)**
- **Efficiency**

May 10, 2016 Ronde Tafel Security



Identified requirements

Reliability

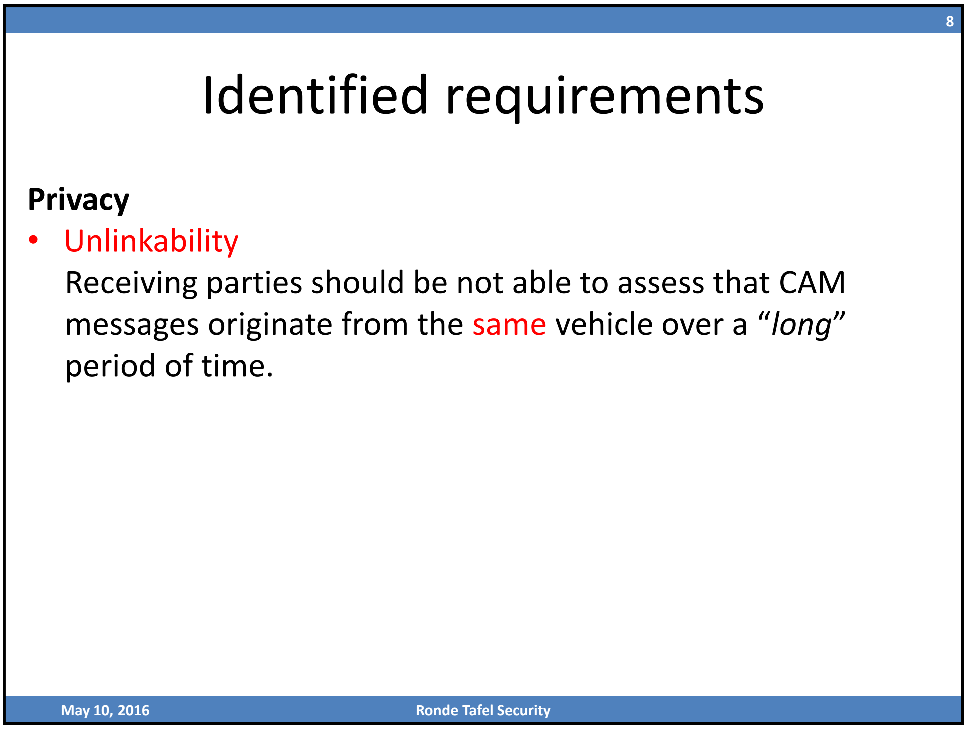
- Authenticity

  Receiving parties should be able to assess that CAM messages originate from a legitimate vehicle.
- Distinguishability

  Receiving parties should be able to reliably identify that CAM messages originate from the same vehicle for a *"short"* time.
- Management of 'misbehaving' vehicles

  There should be a mechanism allowing receiving parties to deal with 'misbehaving' vehicles. Such vehicles need to be identifiable and then removed from the infrastructure after some time.

  Note: revocation of pseudonym certificates is not considered due to huge handling effort (≈ 250 million vehicles in EU).

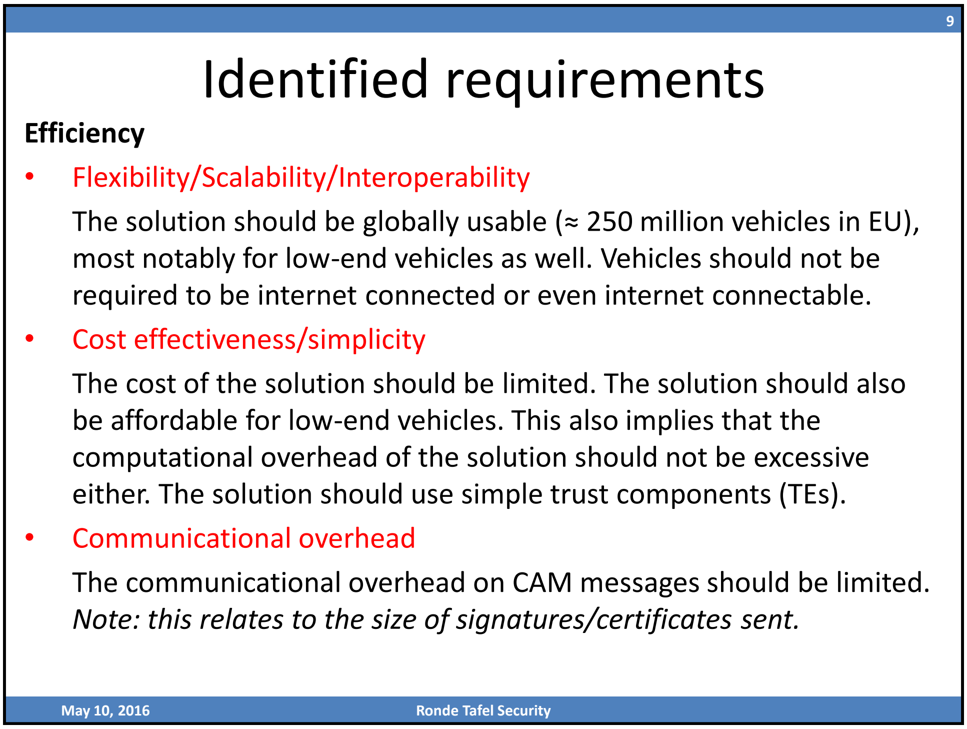


Identified requirements

Privacy

- Unlinkability

  Receiving parties should be not able to assess that CAM messages originate from the same vehicle over a "*long*" period of time.



Identified requirements

Efficiency

- Flexibility/Scalability/Interoperability

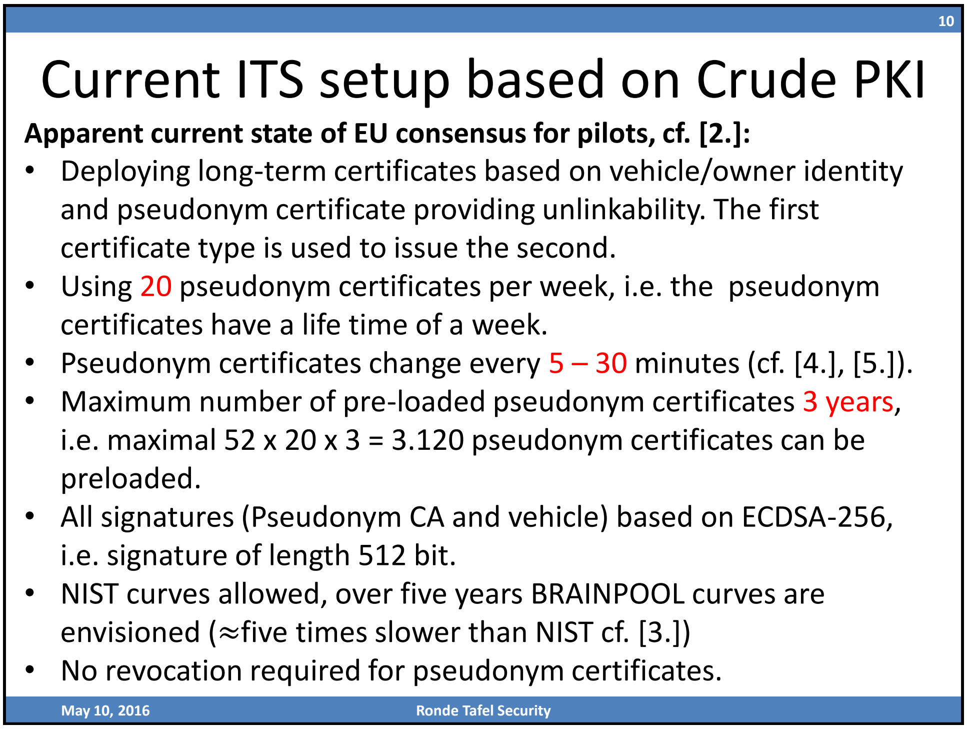
  The solution should be globally usable (≈ 250 million vehicles in EU), most notably for low-end vehicles as well. Vehicles should not be required to be internet connected or even internet connectable.

- Cost effectiveness/simplicity

  The cost of the solution should be limited. The solution should also be affordable for low-end vehicles. This also implies that the computational overhead of the solution should not be excessive either. The solution should use simple trust components (TEs).

- Communicational overhead

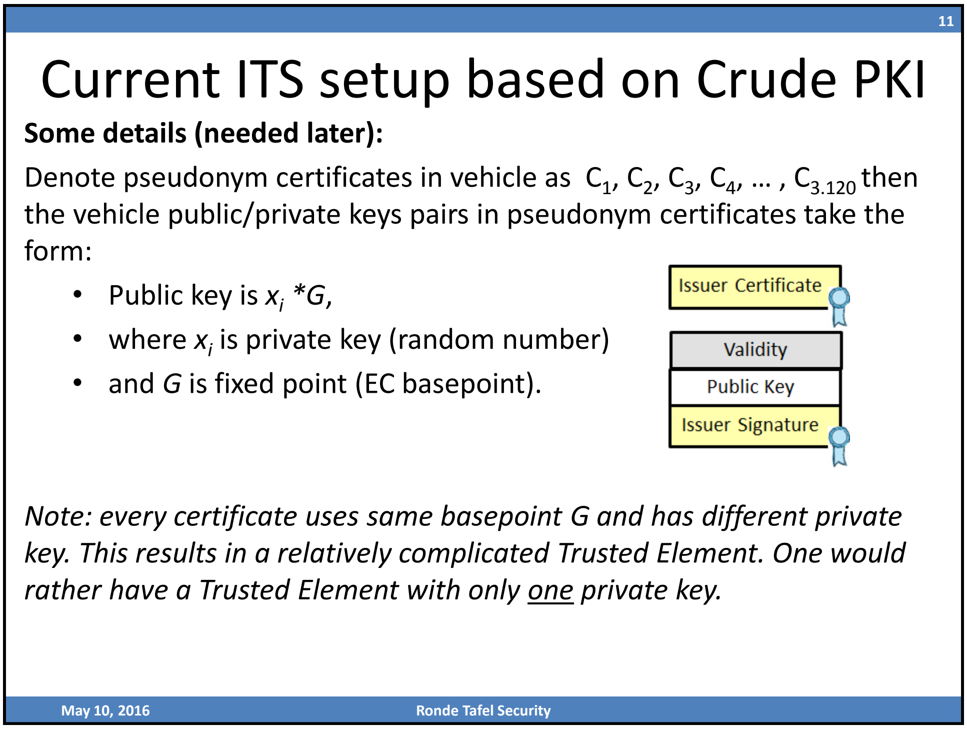
  The communicational overhead on CAM messages should be limited. *Note: this relates to the size of signatures/certificates sent.*



Current ITS setup based on Crude PKI

Apparent current state of EU consensus for pilots, cf. [2.]:

- Deploying long-term certificates based on vehicle/owner identity and pseudonym certificate providing unlinkability. The first certificate type is used to issue the second.
- Using 20 pseudonym certificates per week, i.e. the pseudonym certificates have a life time of a week.
- Pseudonym certificates change every 5 – 30 minutes (cf. [4.], [5.]).
- Maximum number of pre-loaded pseudonym certificates 3 years, i.e. maximal 52 x 20 x 3 = 3.120 pseudonym certificates can be preloaded.
- All signatures (Pseudonym CA and vehicle) based on ECDSA-256, i.e. signature of length 512 bit.
- NIST curves allowed, over five years BRAINPOOL curves are envisioned (≈five times slower than NIST cf. [3.])
- No revocation required for pseudonym certificates.



Current ITS setup based on Crude PKI

Some details (needed later):

Denote pseudonym certificates in vehicle as C_1, C_2, C_3, C_4, … , $C_{3.120}$ then the vehicle public/private keys pairs in pseudonym certificates take the form:

- Public key is x_i *$*G$*,
- where x_i is private key (random number)
- and G is fixed point (EC basepoint).

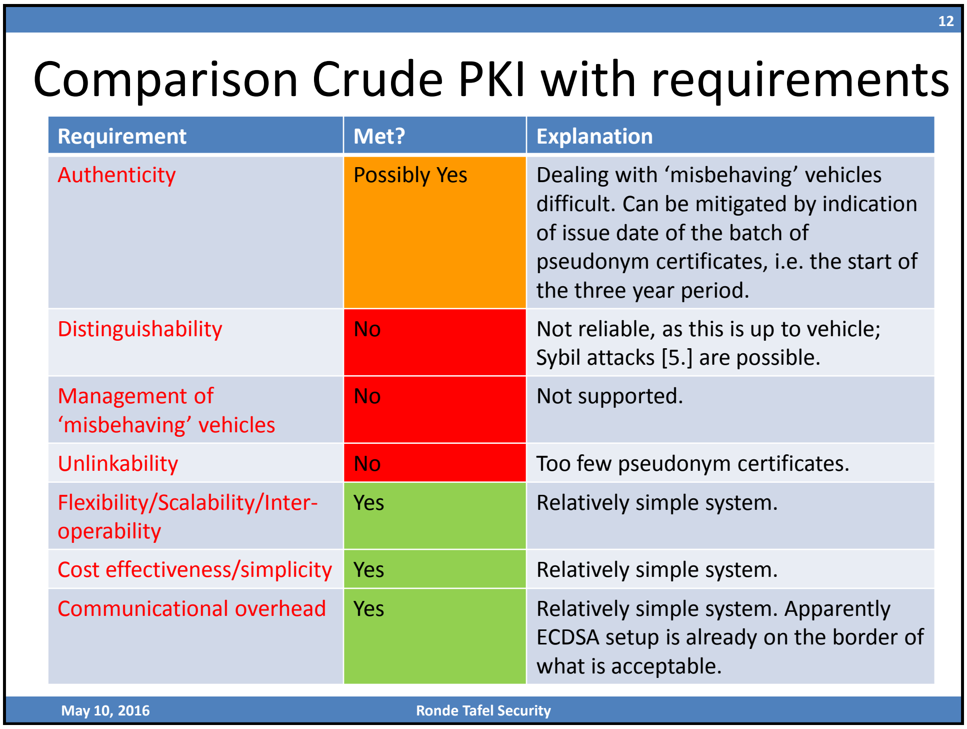
Issuer Certificate

Validity

Public Key

Issuer Signature

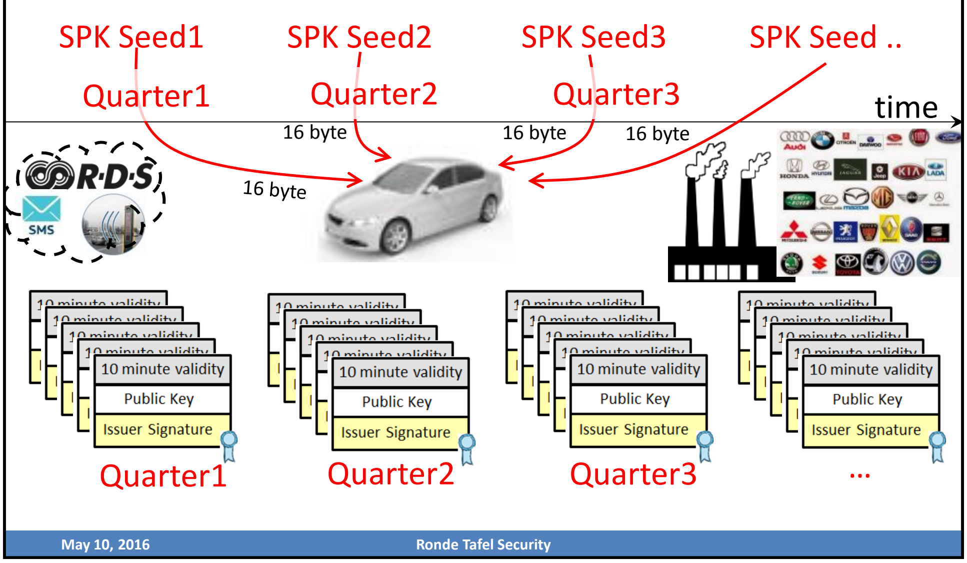
Note: every certificate uses same basepoint G and has different private key. This results in a relatively complicated Trusted Element. One would rather have a Trusted Element with only one private key.



Comparison Crude PKI with requirements

Requirement	Met?	Explanation
Authenticity	Possibly Yes	Dealing with ‘misbehaving’ vehicles difficult. Can be mitigated by indication of issue date of the batch of pseudonym certificates, i.e. the start of the three year period.
Distinguishability	No	Not reliable, as this is up to vehicle; Sybil attacks [5.] are possible.
Management of ‘misbehaving’ vehicles	No	Not supported.
Unlinkability	No	Too few pseudonym certificates.
Flexibility/Scalability/Inter-operability	Yes	Relatively simple system.
Cost effectiveness/simplicity	Yes	Relatively simple system.
Communicational overhead	Yes	Relatively simple system. Apparently ECDSA setup is already on the border of what is acceptable.

Issue first, activate later (IFAL) principle



Issue first, activate later (IFAL) principle

Limited literature analysis did not reveal an obvious issuing principle:

- Issue all pseudonym certificate signatures in advance as part of vehicle manufacturing, e.g. certificates that are only valid for a ten minute period. For 10 years this would mean 10*365*24*6*512 bits ≈ 40 MB, which does not seem excessive. (*) Compare techniques from [11.]
- However, vehicle does not posses corresponding private key(s). These are periodically provided to the vehicle in batches, e.g. quarterly. With straightforward cryptographic techniques this constitutes to quarterly sending only (!) a 128 bit (=16 byte) supplemental private key (SPK) seed value to the vehicle (not secret). This can be done through SMS or broadcasted through the roadside or even through the Radio Data System (RDS). Vehicle owner could also enter the SPK seed manually. *Note: we need GSM/SIMs in new, 'small' vehicles as part of eCall [16.] starting 2018.*
- We could have a certificate indication on SPC seed refreshment period. This could be used by relying parties to assess the reliability of the CAM message: no refreshment is lower reliability of SAM messages.

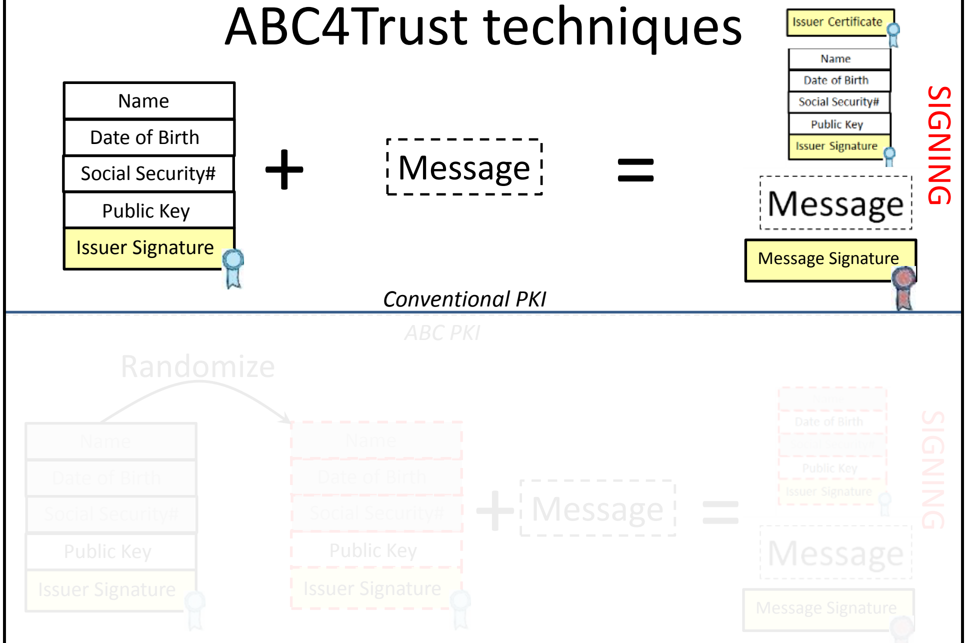
(*) The parameters 10 years, 10 minutes, quarterly refreshment are just examples.

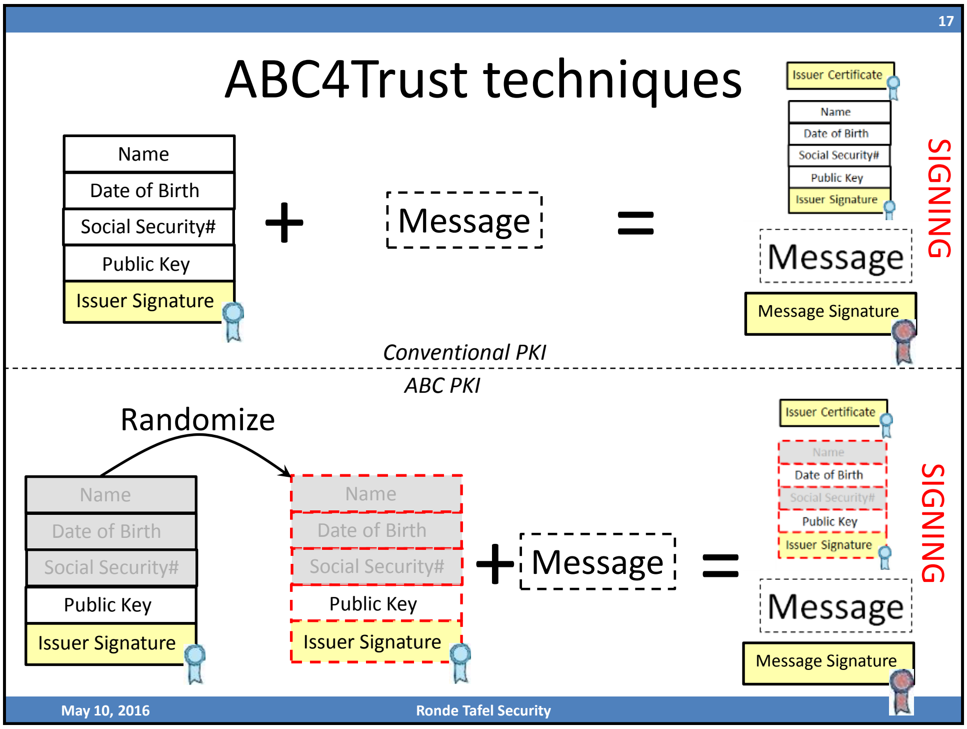
Issue first, activate later (IFAL) principle

- One can easily formulate parametrized IFAL policies giving a balance between Reliability, Privacy (unlinkability) and Efficiency using the three identified parameters: total lifetime, lifetime of certificates, SPC seed refreshment period. This illustrated in the table below in three examples.

Policy#	Reliability	Privacy	Total Lifetime	Cert Lifetime	SPS seed Refresh
1.	High	High	10 years	1 minute	Daily
2.	Medium	Medium	10 years	10 minutes	Quarterly
3.	Low	Low	10 years	1 hour	10 years
4.	..	..	..	..	..

ABC4Trust techniques





ABC4Trust techniques

Name
Date of Birth
Social Security#
Public Key
Issuer Signature

+ Message =

Issuer Certificate
Name
Date of Birth
Social Security#
Public Key
Issuer Signature
Message
Message Signature

SIGNING

Conventional PKI

ABC PKI

Randomize

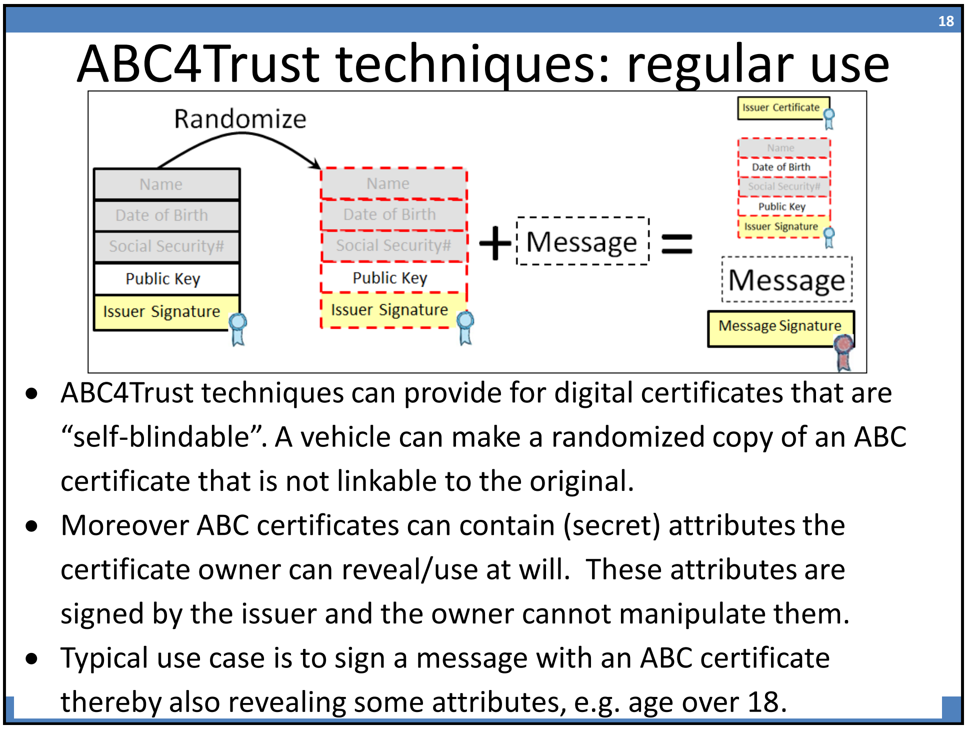
Name
Date of Birth
Social Security#
Public Key
Issuer Signature

Name
Date of Birth
Social Security#
Public Key
Issuer Signature

+ Message =

Issuer Certificate
Name
Date of Birth
Social Security#
Public Key
Issuer Signature
Message
Message Signature

SIGNING



ABC4Trust techniques: regular use

Randomize

Name
Date of Birth
Social Security#
Public Key
Issuer Signature

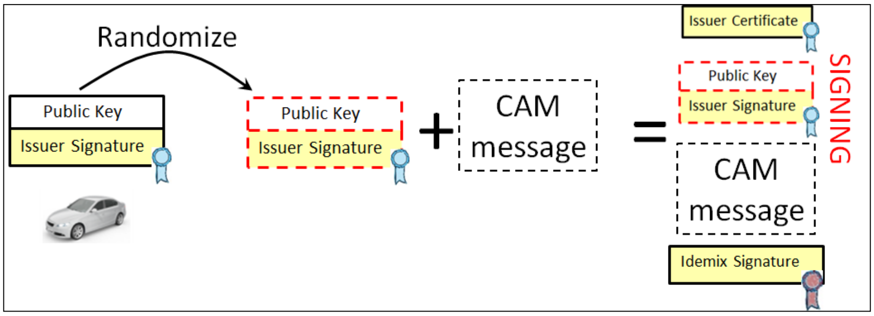
Name
Date of Birth
Social Security#
Public Key
Issuer Signature

+ Message =

Issuer Certificate
Name
Date of Birth
Social Security#
Public Key
Issuer Signature
Message
Message Signature

- ABC4Trust techniques can provide for digital certificates that are “self-blindable”. A vehicle can make a randomized copy of an ABC certificate that is not linkable to the original.
- Moreover ABC certificates can contain (secret) attributes the certificate owner can reveal/use at will. These attributes are signed by the issuer and the owner cannot manipulate them.
- Typical use case is to sign a message with an ABC certificate thereby also revealing some attributes, e.g. age over 18.

ABC4Trust techniques: first idea



Randomize

Public Key

Issuer Signature

Public Key

Issuer Signature

+

CAM message

=

Issuer Certificate

Public Key

Issuer Signature

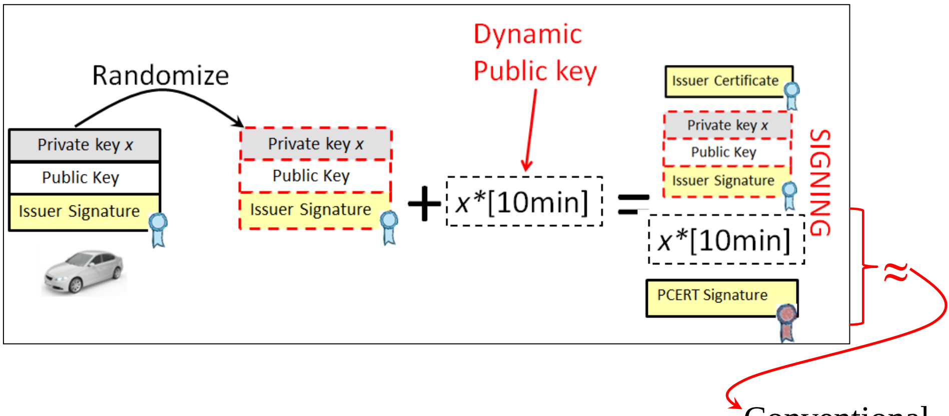
CAM message

Idemix Signature

SIGNING

This setup would contradict Distinguishability.

ABC4Trust techniques: suggested setup



Randomize

Private key x

Public Key

Issuer Signature

Private key x

Public Key

Issuer Signature

+

Dynamic Public key

x*[10min]

=

Issuer Certificate

Private key x

Public Key

Issuer Signature

x*[10min]

PCERT Signature

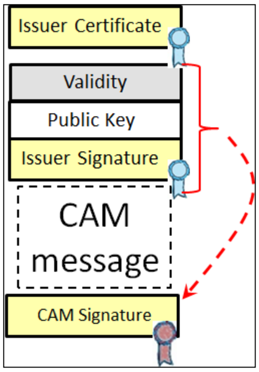
SIGNING

≈

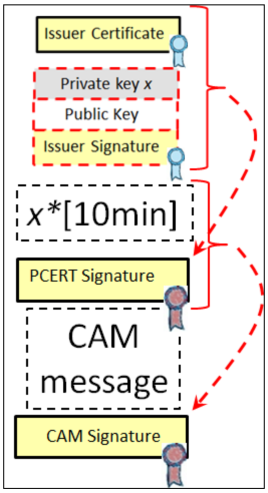
Conventional pseudonym certificate

That is, create your own 10 minute valid pseudonym certificates….

ABC4Trust techniques: comparison

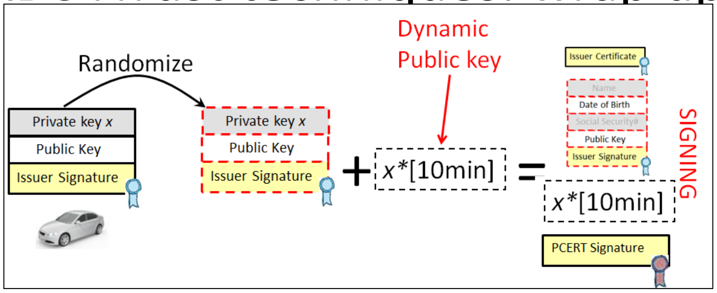


Conventional setup



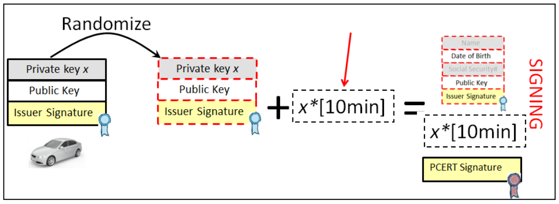
Suggested Idemix setup

ABC4Trust techniques: wrap up



- ITS application would be to put a secret attribute *x* (hidden) in an ABC certificate and to periodically generate your own pseudonym certificates. Pseudonym CA is effectively made obsolete.
- The vehicle public keys inside these pseudonym certificates would be slightly different: the private key would always be equal, but the basepoint would correspond with a 10 minute time period enforcing Distinguishability. This is a common ABC construction called domain pseudonyms in [6.].
- Using no domain pseudonyms would contradict Distinguishability.

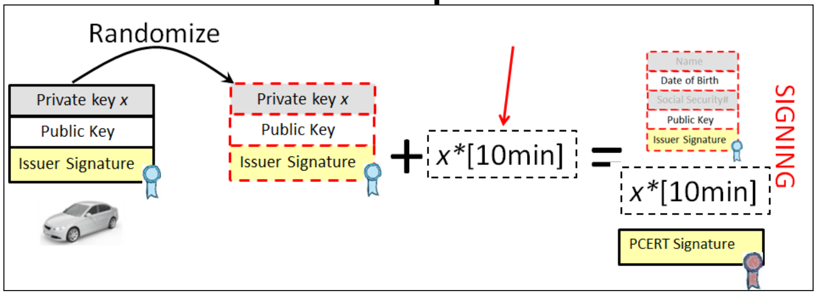
ABC4Trust techniques: efficiency



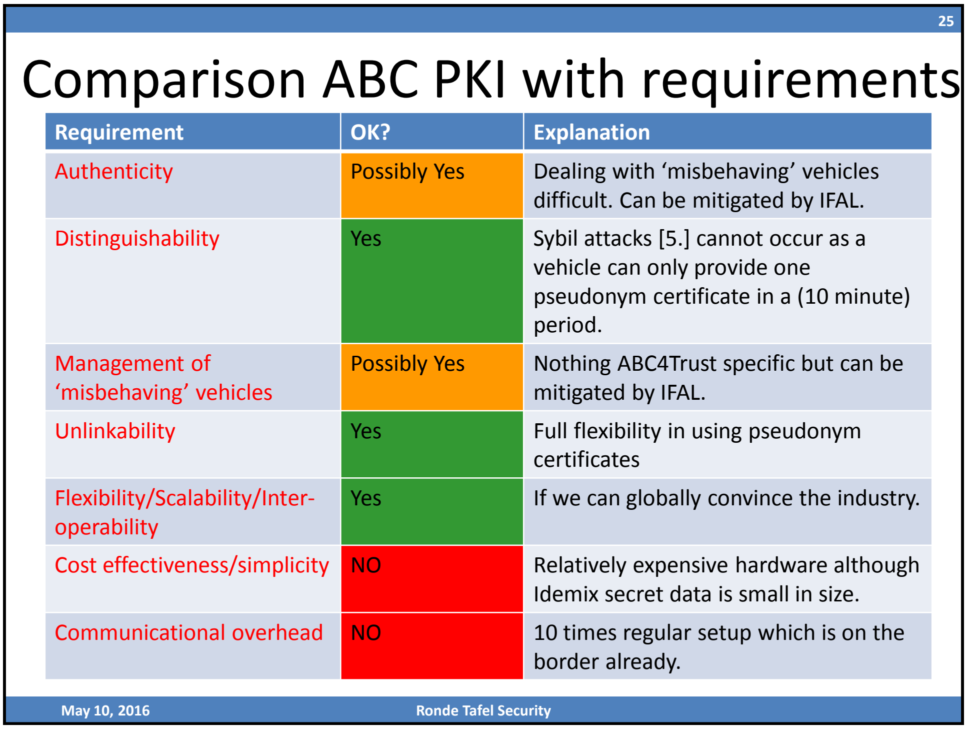
Using Idemix [10.] (best known ABC technique based on RSA):

- one RANDOMIZE + SIGN Idemix (RSA2048) operation is at least 350 times slower than NIST ECDSA-256 signing and 70 times slower than BRAINPOOL ECDSA-256 signing.
- One Idemix VERIFICATION (RSA2048) operation is at least 60 times slower than NIST ECDSA-256 verification and 12 times slower than BRAINPOOL ECDSA-256 verification.
- Size of Idemix certificate is 10 times the size of a ECDSA certificate.
- Data size in vehicle is about 1 KB for each IFAL period corresponding to 0,1*#(p_certs) KB in conventional setup (few MB)

ABC4Trust techniques: revocation

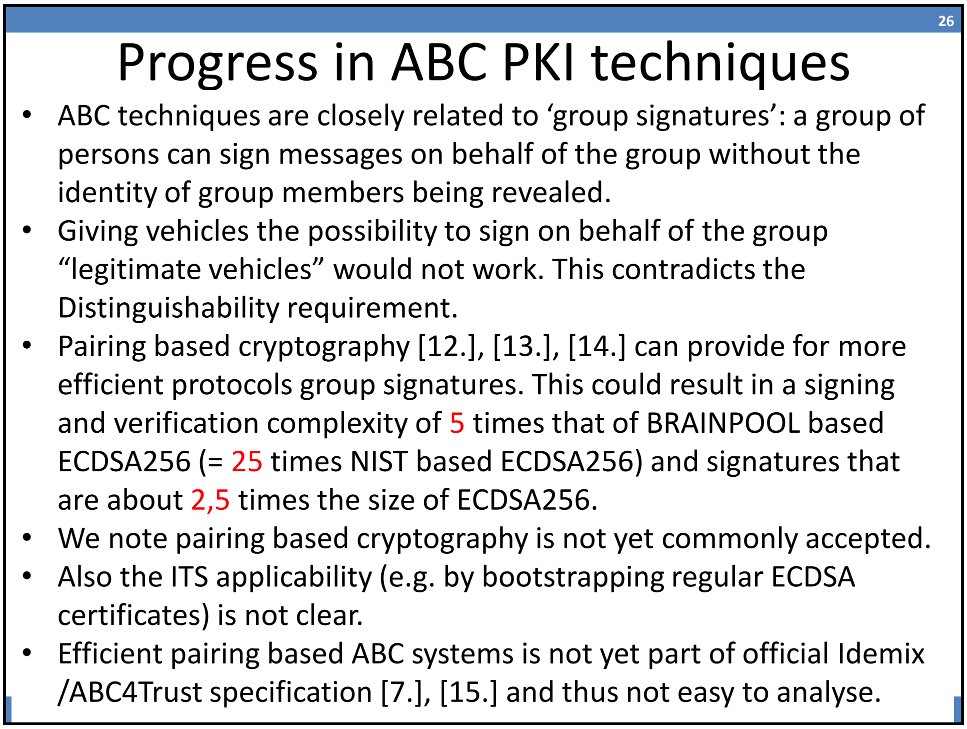


- Idemix has revocation techniques but these are more complex then regular pseudonym certificate revocation: extra non trivial computational work at both the sending vehicle and receiving party.
- As revocation is not considered for pseudonym certificate revocation we also do not consider it in Idemix application either.



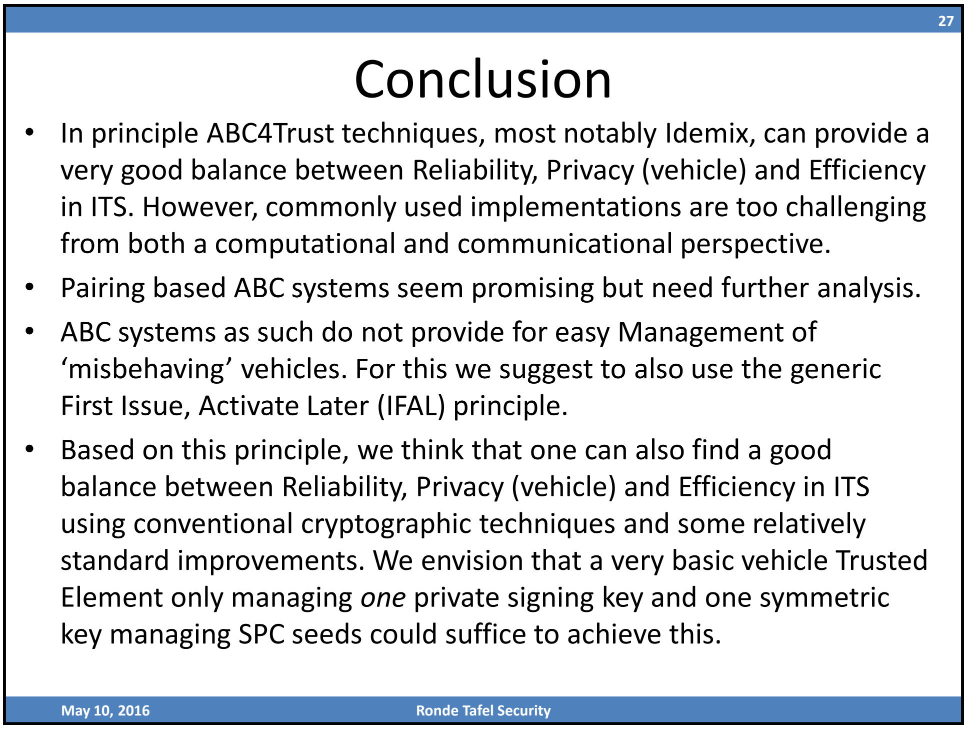
Comparison ABC PKI with requirements

Requirement	OK?	Explanation
Authenticity	Possibly Yes	Dealing with ‘misbehaving’ vehicles difficult. Can be mitigated by IFAL.
Distinguishability	Yes	Sybil attacks [5.] cannot occur as a vehicle can only provide one pseudonym certificate in a (10 minute) period.
Management of ‘misbehaving’ vehicles	Possibly Yes	Nothing ABC4Trust specific but can be mitigated by IFAL.
Unlinkability	Yes	Full flexibility in using pseudonym certificates
Flexibility/Scalability/Inter-operability	Yes	If we can globally convince the industry.
Cost effectiveness/simplicity	NO	Relatively expensive hardware although Idemix secret data is small in size.
Communicational overhead	NO	10 times regular setup which is on the border already.



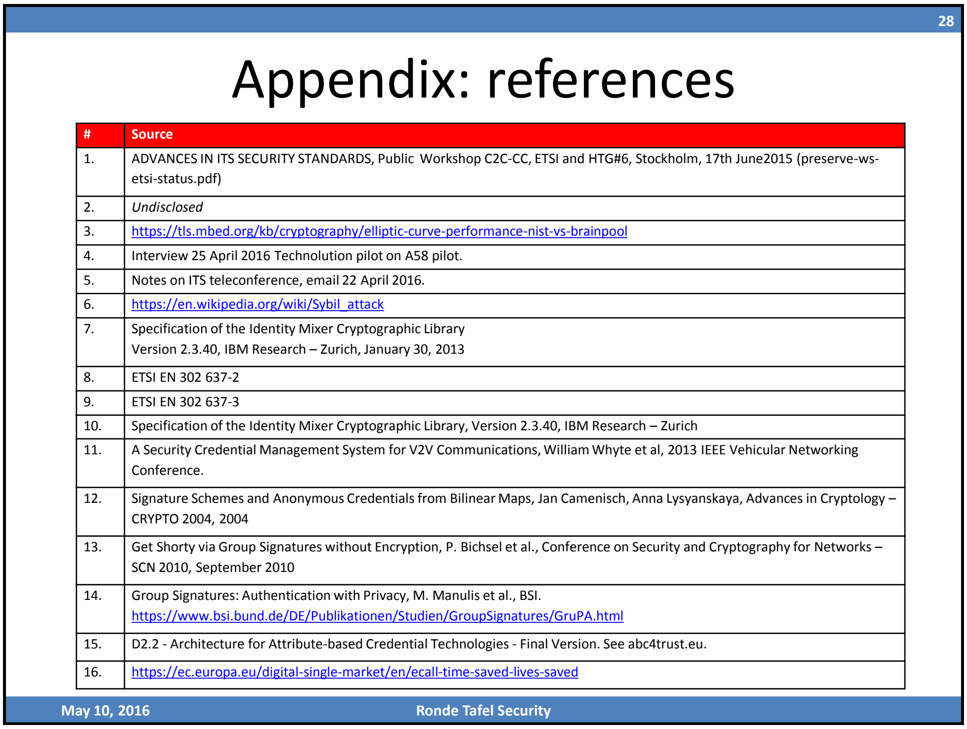
Progress in ABC PKI techniques

- ABC techniques are closely related to ‘group signatures’: a group of persons can sign messages on behalf of the group without the identity of group members being revealed.
- Giving vehicles the possibility to sign on behalf of the group “legitimate vehicles” would not work. This contradicts the Distinguishability requirement.
- Pairing based cryptography [12.], [13.], [14.] can provide for more efficient protocols group signatures. This could result in a signing and verification complexity of 5 times that of BRAINPOOL based ECDSA256 (= 25 times NIST based ECDSA256) and signatures that are about 2,5 times the size of ECDSA256.
- We note pairing based cryptography is not yet commonly accepted.
- Also the ITS applicability (e.g. by bootstrapping regular ECDSA certificates) is not clear.
- Efficient pairing based ABC systems is not yet part of official Idemix /ABC4Trust specification [7.], [15.] and thus not easy to analyse.



Conclusion

- In principle ABC4Trust techniques, most notably Idemix, can provide a very good balance between Reliability, Privacy (vehicle) and Efficiency in ITS. However, commonly used implementations are too challenging from both a computational and communicational perspective.
- Pairing based ABC systems seem promising but need further analysis.
- ABC systems as such do not provide for easy Management of 'misbehaving' vehicles. For this we suggest to also use the generic First Issue, Activate Later (IFAL) principle.
- Based on this principle, we think that one can also find a good balance between Reliability, Privacy (vehicle) and Efficiency in ITS using conventional cryptographic techniques and some relatively standard improvements. We envision that a very basic vehicle Trusted Element only managing *one* private signing key and one symmetric key managing SPC seeds could suffice to achieve this.



Appendix: references

#	Source
1.	ADVANCES IN ITS SECURITY STANDARDS, Public Workshop C2C-CC, ETSI and HTG#6, Stockholm, 17th June2015 (preserve-ws-etsi-status.pdf)
2.	*Undisclosed*
3.	https://tls.mbed.org/kb/cryptography/elliptic-curve-performance-nist-vs-brainpool
4.	Interview 25 April 2016 Technolution pilot on A58 pilot.
5.	Notes on ITS teleconference, email 22 April 2016.
6.	https://en.wikipedia.org/wiki/Sybil_attack
7.	Specification of the Identity Mixer Cryptographic Library Version 2.3.40, IBM Research – Zurich, January 30, 2013
8.	ETSI EN 302 637-2
9.	ETSI EN 302 637-3
10.	Specification of the Identity Mixer Cryptographic Library, Version 2.3.40, IBM Research – Zurich
11.	A Security Credential Management System for V2V Communications, William Whyte et al, 2013 IEEE Vehicular Networking Conference.
12.	Signature Schemes and Anonymous Credentials from Bilinear Maps, Jan Camenisch, Anna Lysyanskaya, Advances in Cryptology – CRYPTO 2004, 2004
13.	Get Shorty via Group Signatures without Encryption, P. Bichsel et al., Conference on Security and Cryptography for Networks – SCN 2010, September 2010
14.	Group Signatures: Authentication with Privacy, M. Manulis et al., BSI. https://www.bsi.bund.de/DE/Publikationen/Studien/GroupSignatures/GruPA.html
15.	D2.2 - Architecture for Attribute-based Credential Technologies - Final Version. See abc4trust.eu.
16.	https://ec.europa.eu/digital-single-market/en/ecall-time-saved-lives-saved