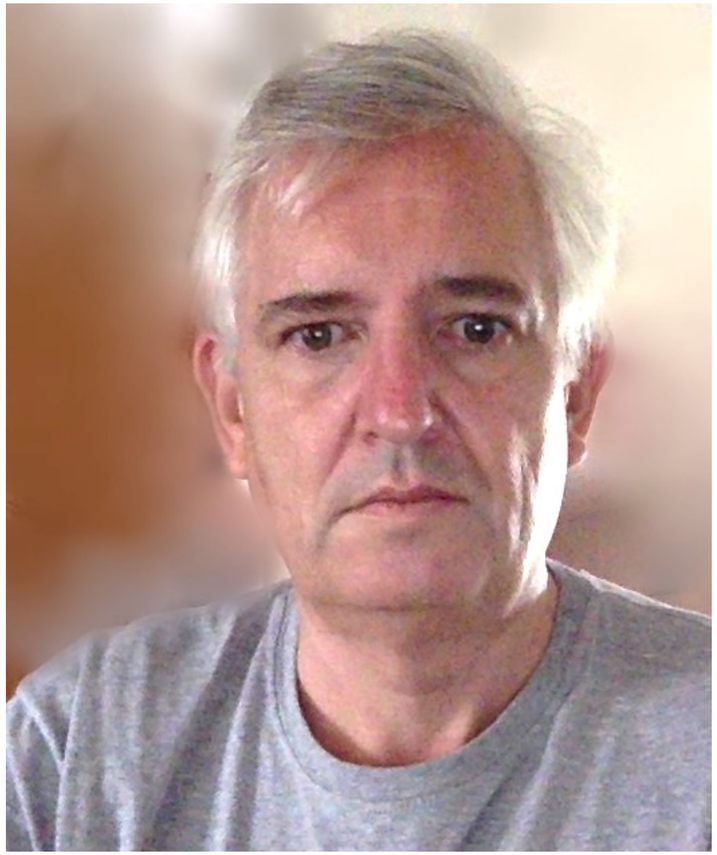
ITS Standards: Key enabling technologies

Cybersecurity

Scott CADZOW, 12th January 2021

Core topics

What is security?
Usage of IEEE 1609.2 for (1) signing of messages, (2) secure sessions.
Access control.



Introduction

… and an agenda of sorts

In the context of ITS, Cybersecurity refers to the mitigation of attacks on the system, or elements of the system.

System elements are primarily the ITS-S and its communications payload

Security provisions are somewhat fractal in nature - the same abstractions at any level of magnification of the system

Security is **not** about certificates, but they are important

Security – *some* definitions (noun)

… what is security?

- the state of being free from danger or injury
- a formal declaration that documents a fact of relevance to finance and investment
- a department responsible for the security of the institution's property and workers
- measures taken as a precaution against theft or espionage or sabotage etc.
- defence against financial failure
- freedom from anxiety or fear
- property that your creditor can claim in case you default on your obligation
- a guarantee that an obligation will be met
- …

Safety deals with …

Health & Wellbeing

- Will I suffer (physically/mentally) from doing this activity?
- Will others suffer from my doing this activity?

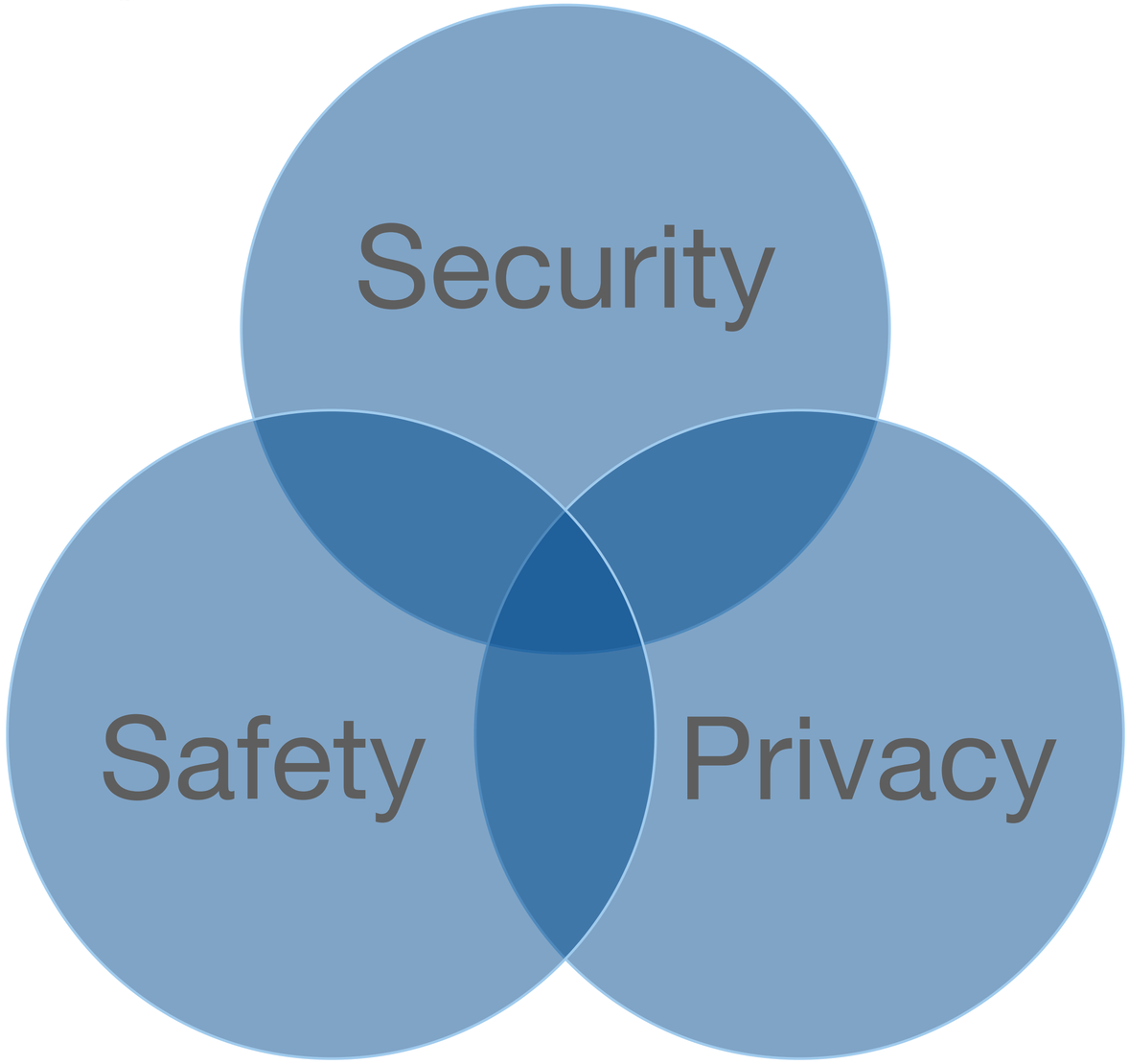
Security deals with …

The things we think of that make us feel safe

- Details to lead to safety - Integrity
- Checking who people are - Authenticity
- Checking people are allowed to do things - Authority
- Keeping their communication confidential - Confidentiality

The intersection concern

Mitigations and subject matter intersect



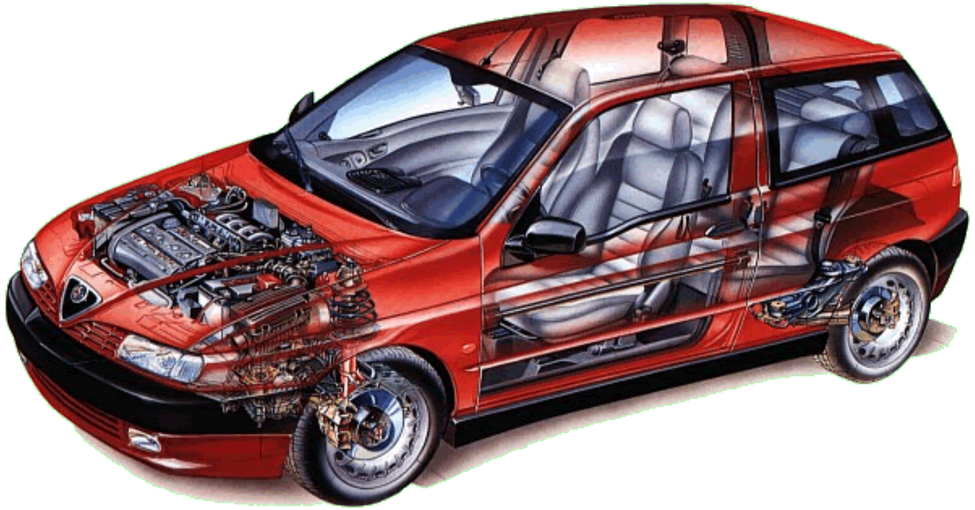
Conventional transport industry measures

Security in the sense of safety

Automotive industry

- NCAP ratings
  - Number of airbags
  - Crumple zones
  - Intrusion prevention
  - Protection of passengers
  - Protection of pedestrians
  - Protection of other drivers
- Active and passive safety
  - Roadholding
  - Handling
  - Noise, Vibration, Harshness (NVH)
  - ABS, EBA, ETC, …

Some cybersecurity tests are being added into Type Approval



Scalability of security solutions

This is the first dimension to understand

Easy to keep a secret with two parties?

- Basis of symmetric key cryptology

Impossible to keep a secret with more than 3 parties?

- Basis of asymmetric key cryptology (Ellis of UK CESG proposed Non-Secret Encryption in 1970)

Scenarios:

- Correspondents know and trust one another and the network
- Correspondents know and trust one another but don't trust the network
- Correspondents know but don't trust one another but trust the network - **The target in ITS**
- Correspondents don't know one another - **This is the C-ITS model**
- Communications network is public - **The core model for ITS**
- Communications network is private

Security capabilities

Our mitigation toolkit

Primary capabilities

- Confidentiality
- Integrity
- Authenticity
- Authority

Secondary capabilities

- Availability
- Reliability
- Repeatability

Enabled by

Cryptology

- The mathematical means

Key management

- Key association
- Key revocation
- Key renewal
- Key transfer

Core lessons to learn

Subtle knowledge

- **Kerchoff's principle**: A cryptosystem should be secure even if everything about the system, except the key, is public knowledge
- **Shannon's restatement**: "the enemy knows the system", i.e., "one ought to design systems under the assumption that the enemy will immediately gain full familiarity with them"
- **Generalisation**: The fewer and simpler the secrets that one must keep to ensure system security, the easier it is to maintain system security.

Security philosophy

Why open is good

Open security versus closed:

- **Schneier**: Every secret creates a potential failure point. Secrecy, in other words, is a prime cause of brittleness—and therefore something likely to make a system prone to catastrophic collapse. Conversely, openness provides ductility

- **Bellovin**: Design your system assuming that your opponents know it in detail. After that, though, there's nothing wrong with trying to keep it secret – it's another hurdle the enemy has to overcome.

Trust, security, privacy

ITS is a trust based system

- Trust is defined as confidence in the integrity of an entity for reliance on that entity to fulfil specific responsibilities.
  - Trust is highly dynamic and contextual, and may be described in assurance levels based on specific measures that identify when and how a relationship or transaction can be relied upon.
  - Trust measures can combine a variety of elements that include identity, attribution, attestation and non-repudiation.
  - Multiple models for trust networks exist for ITS
- The core requirement related to trust in any system is the identification of the "root of trust".
  - For each element protected within a trust relationship it is necessary to identify both the root of trust and the path from the protected element to the root of trust.

Some myths or commonly ignored features about trust

- Having a secured communications channel with another entity is never sufficient reason to trust that entity, even if you trust the underlying security primitives on which that communications channel is based.
- Trust is not a binary operation. There may be various levels of trust that an entity has for another.
- Trust may be relative, not absolute.
  - Entity A may trust Entity C more than Entity B, without trusting either absolutely.
- Trust is rarely symmetric. Entity A may trust Entity B completely, whereas the amount of trust that B has for A may be very low.
  - This does not always matter: a schoolchild may trust a schoolteacher, for instance, without any requirement for that trust to be reciprocated.
- One of the axes for trust is time, and the trust relationship between two entities may be highly dynamic over time.
  - Just because a certain level of trust was established at point T, it does not mean that that level will be maintained at time T+ τ, as it can increase and decrease.

The role of standards in ITS security

- Framework for deploying trust
- Bob trusts the data he gets from Alice because Charles says its ok
  - Bob is the receiving entity, Alice is the requesting entity, and Charles is the shared trusted party
- Alice demonstrates trust by signing data where his signature is verified as authentic by Charles
  - Bob has confidence (trust) that Charles will not arbitrarily verify/notarise Alice

Digital signature and certificates

- A public key certificate:
  - Holds the public key associated to a specific private key
  - Has an attestation by a trusted party of the public-private key association
- A digital signature encrypts data (usually a hash) with the private key
- A digital signature is verified by using the public key to “prove” the data can only have been encrypted by the matching private key

Forms of certificate

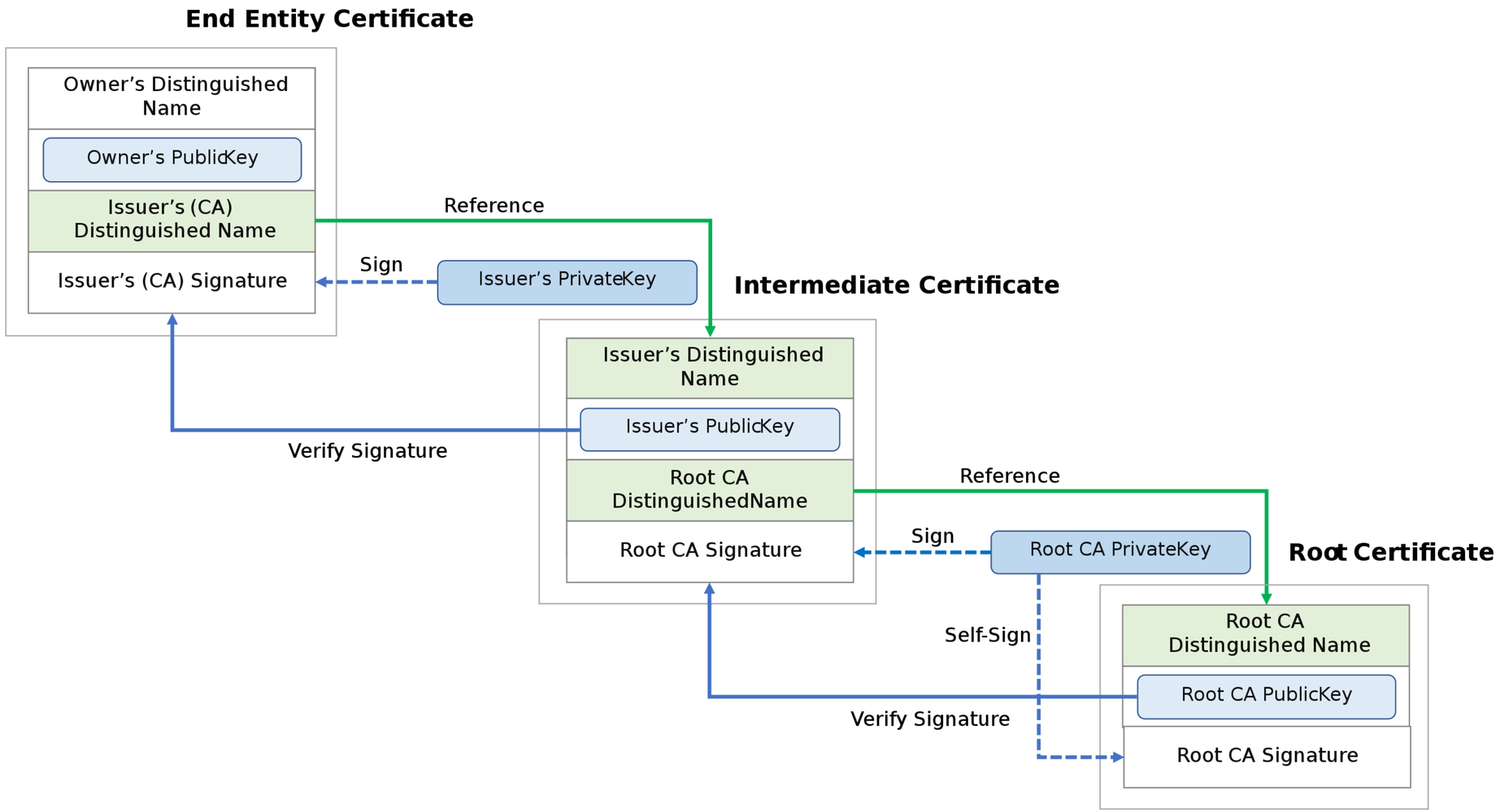
- Identity certificates
  - Attest to the identity of the holder (the key pair is bound to the identity)
  - Public key is used in authentication of the identity (e.g. in data signature)
- Attribute certificates
  - Attest to certain attributes of the holder (the key pair is bound to the attribute)

Certificate standards

Not many standards, lots of applications

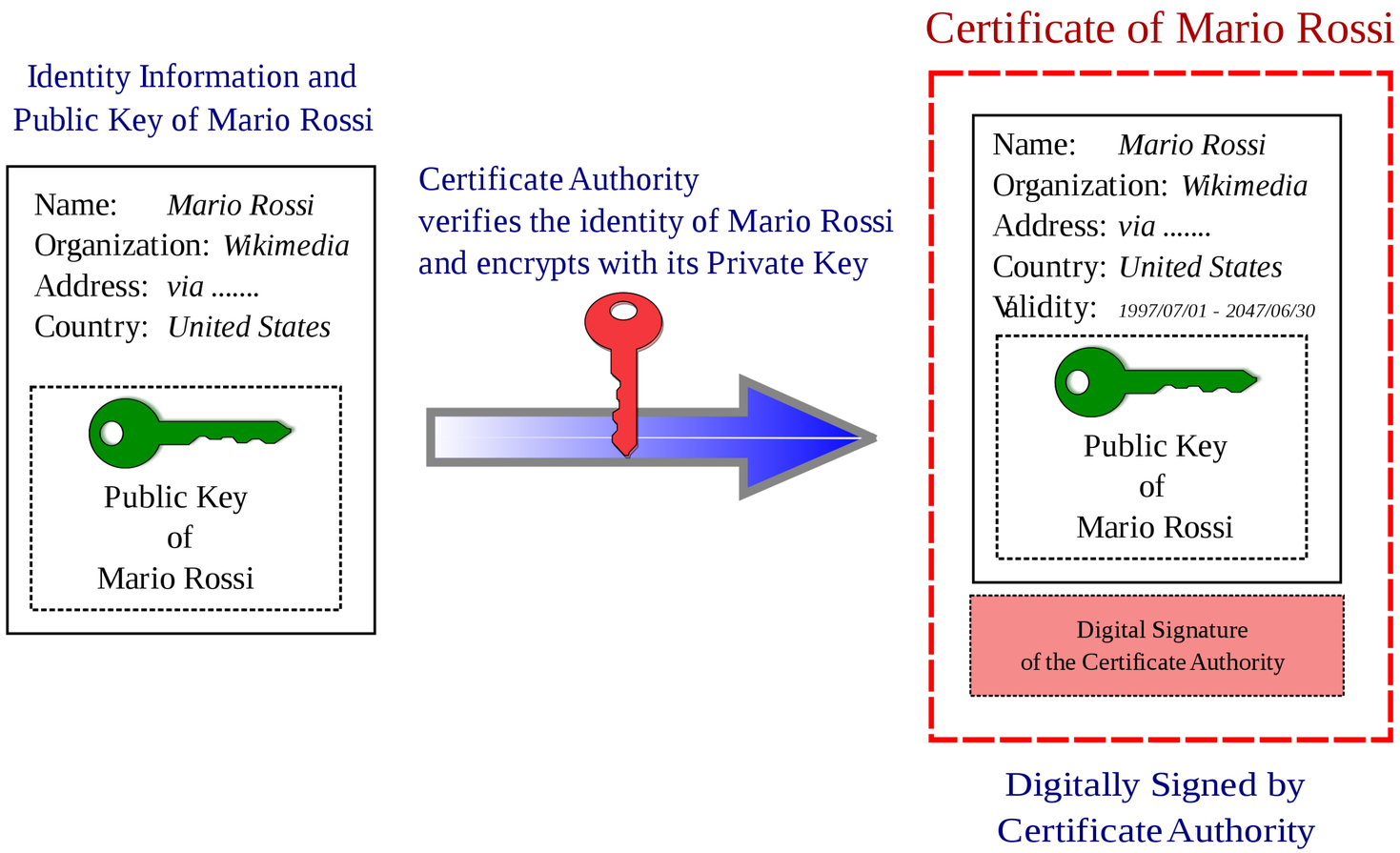
- ITU-T X.509
  - Allows both identity and attribute (linked) certificates
  - Verbose, linked to most e-commerce and signature schemes
- IEEE 1609.2
  - Predominately an attribute certificate - optimised for ITS applications
  - Encodes permissions (the SSP field)

Certificate chain in trust networks



Certificates in identity

Attestation by the CA of the data offered by the holder



ITS standards

- A multi-authority trust model (enabled already in the EU for C-ITS)
- An efficient attribute based security model using IEEE 1609.2
- An expandable identity based security model using X.509
- A single operational security model defined in ISO 21177 (building on other activity in ISO, CEN, IEEE and ETSI)