escrypt
SECURITY. TRUST. SUCCESS.

Creating Trusted Data to Enable ITS Applications in Smart Cities

Kevin Henry
ESCRYPT Canada

Overview

escrypt
SECURITY. TRUST. SUCCESS.

- Smart City Data Model
- Transportation Example
- Value of Trusted Data
- Shared Sensors and Cross-Domain Data
- Public Key Infrastructure (PKI) and Trusted Data
- Smart City Complexity

Smart City Data Model

Focus on data flow and decision processing

escrypt
SECURITY. TRUST. SUCCESS.

- It is difficult to define a “Smart City”
  - Means different things to different people
  - Many potential use-cases and value propositions
  - Multiple integration points
- To understand smart city security models, we can focus on data flows and decision processing

Smart City Data Model

Select examples of basic use cases

escrypt
SECURITY. TRUST. SUCCESS.

- Fortunately, we do not need an expansive definition
- Look at a few representative examples:

Example: Use a strain gauge for early detection of cracks or wear on a bridge or building

http://www.vistadatavision.com/portfolio-item/long-term-monitoring-reinforced-concrete-highway-bridge-university-sao-paulo/

Example: Use a traffic camera to monitor vehicle and pedestrian traffic, adjust signals to improve pedestrian safety

https://www.bhphotovideo.com/c/product/1274692-REG/bosch_vkn_5085v4_20_outdoor_prepackaged_camera_dinion.html

Example: Monitor public infrastructure and efficiently direct repair crews to perform preventive maintenance

http://www.wabi.tv/content/news/City-of-Brewer-set-to-begin-street-light-conversion-project-479201053.html

Smart City Data Model

Simple data model captures most common use-cases

escrypt
SECURITY. TRUST. SUCCESS.

- By focusing on data flow, a simple repeating pattern emerges
  - Central to nearly all connected, smart city use cases is the flow of data from a data acquisition module or sensor, to an analysis function, resulting in some action or report
  - Security is needed for this chain is to produce an actionable and trusted outcome

In order to produce meaningful results, the whole chain must be trusted

  - Integrity of the internal network for core infrastructure and decision making must be maintained while at the same time a multitude of new, low-cost sensors are added
  - Trust becomes even more critical if a single sensor is to be used for more than one application

Transportation Example

Video detection of vehicles and pedestrians

escrypt
SECURITY. TRUST. SUCCESS.

- Modern video systems can provide automated analytics that can count cars, monitor flow rates, and even detect pedestrians, pets, and bicycles
- The same video feed can be used for additional use cases
  - Security monitoring of store-fronts near an intersection
  - Monitoring of infrastructure and road surface conditions
  - Tracking of transit vehicles against a schedule
  - Police investigations
  - Etc.

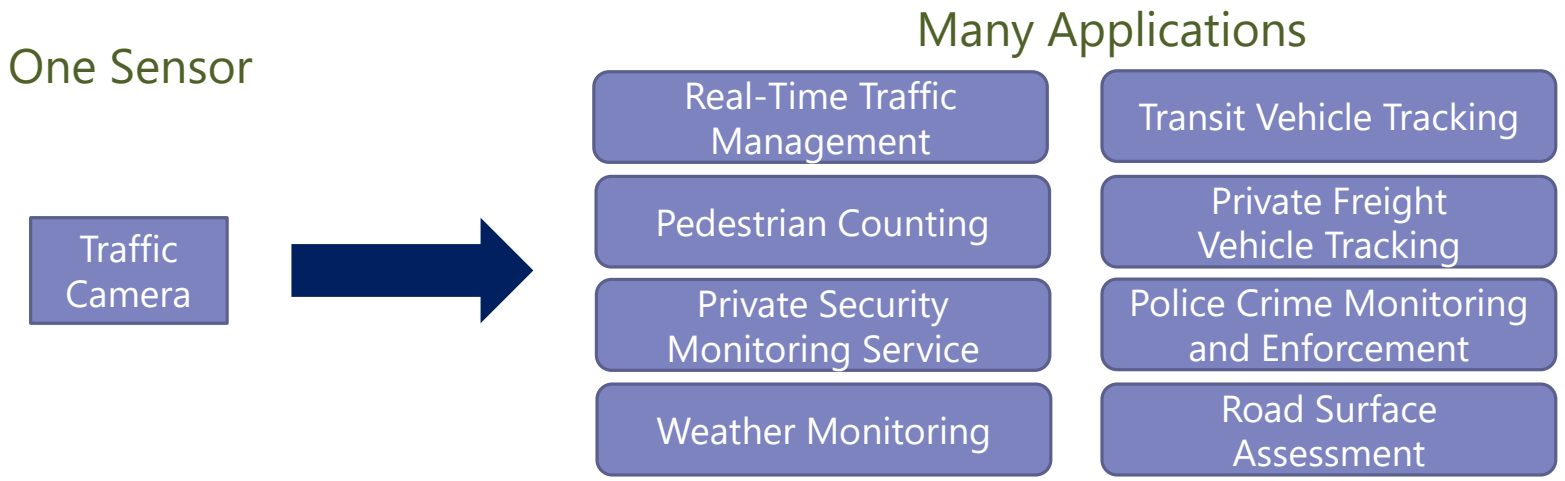
https://www.youtube.com/watch?v=Z7j1hziLY4k

Transportation Example

Trusted data distribution

escrypt
SECURITY. TRUST. SUCCESS.

- What happens when one sensor is used for multiple applications?
  - Who "owns" the sensor and repairs it if it fails?
  - Can data be safely shared across different city departments?
  - Was the data modified by some other application before it was delivered for analysis?
- To fully realize the value of smart city deployments, we need to fully exploit the value of each sensor for multiple applications



Value of Trusted Data

Trust the data, not the network

escrypt
SECURITY. TRUST. SUCCESS.

- In order for data to be useful, it must be trusted
  - Need confidence that data is fresh, not replayed or modified
  - Need confidence that data will be available when needed
- In order to maintain service, both sensors and applications need protection
  - Need to protect the sensor from rogue actors
  - Need to protect applications from network attacks

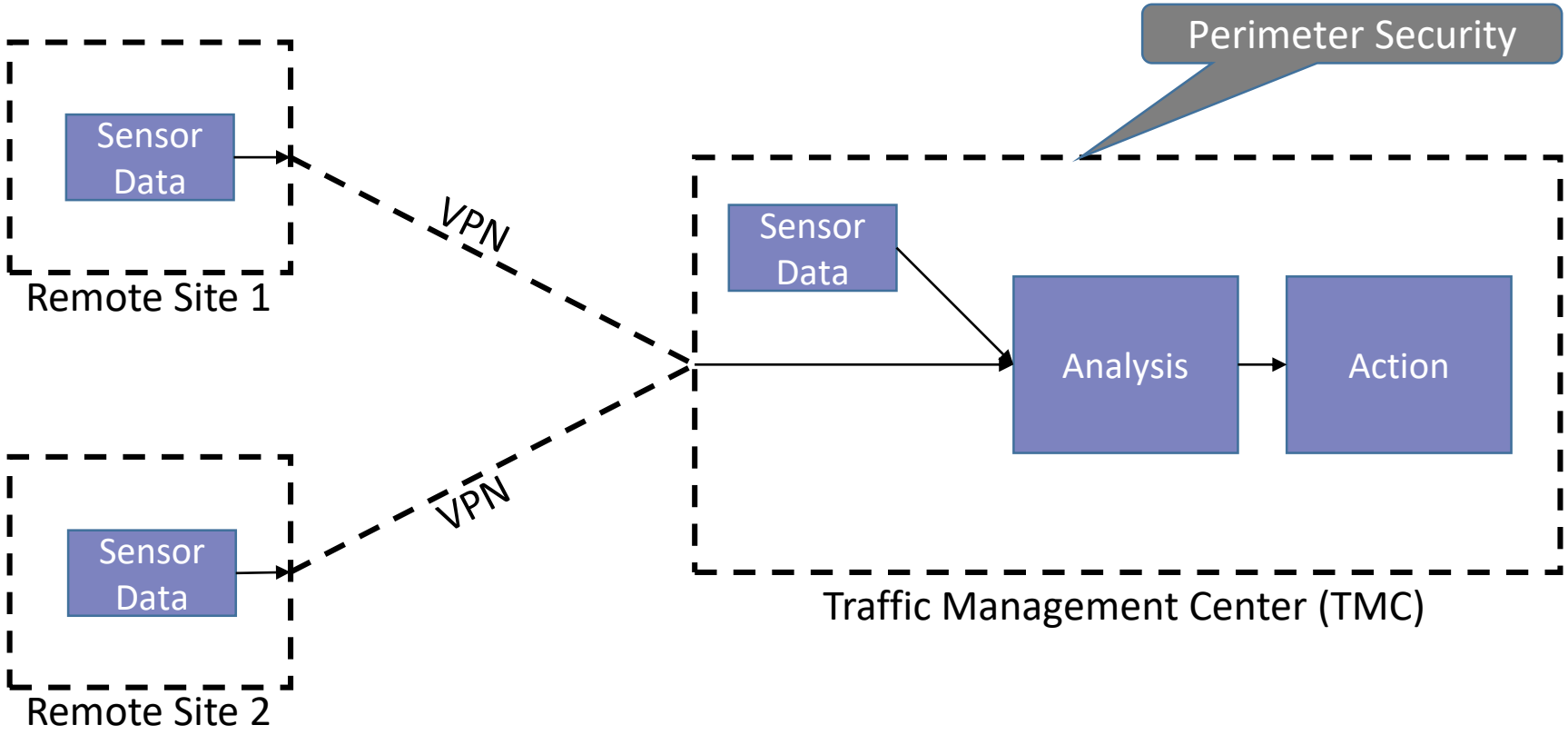
- Typical approach to ensuring trust in the data is to require a trusted network
  - This is complex and expensive and doesn't scale well

Value of Trusted Data

Secure networks are hard to support at scale

escrypt
SECURITY. TRUST. SUCCESS.

- Extending perimeter security to remote devices does not scale well

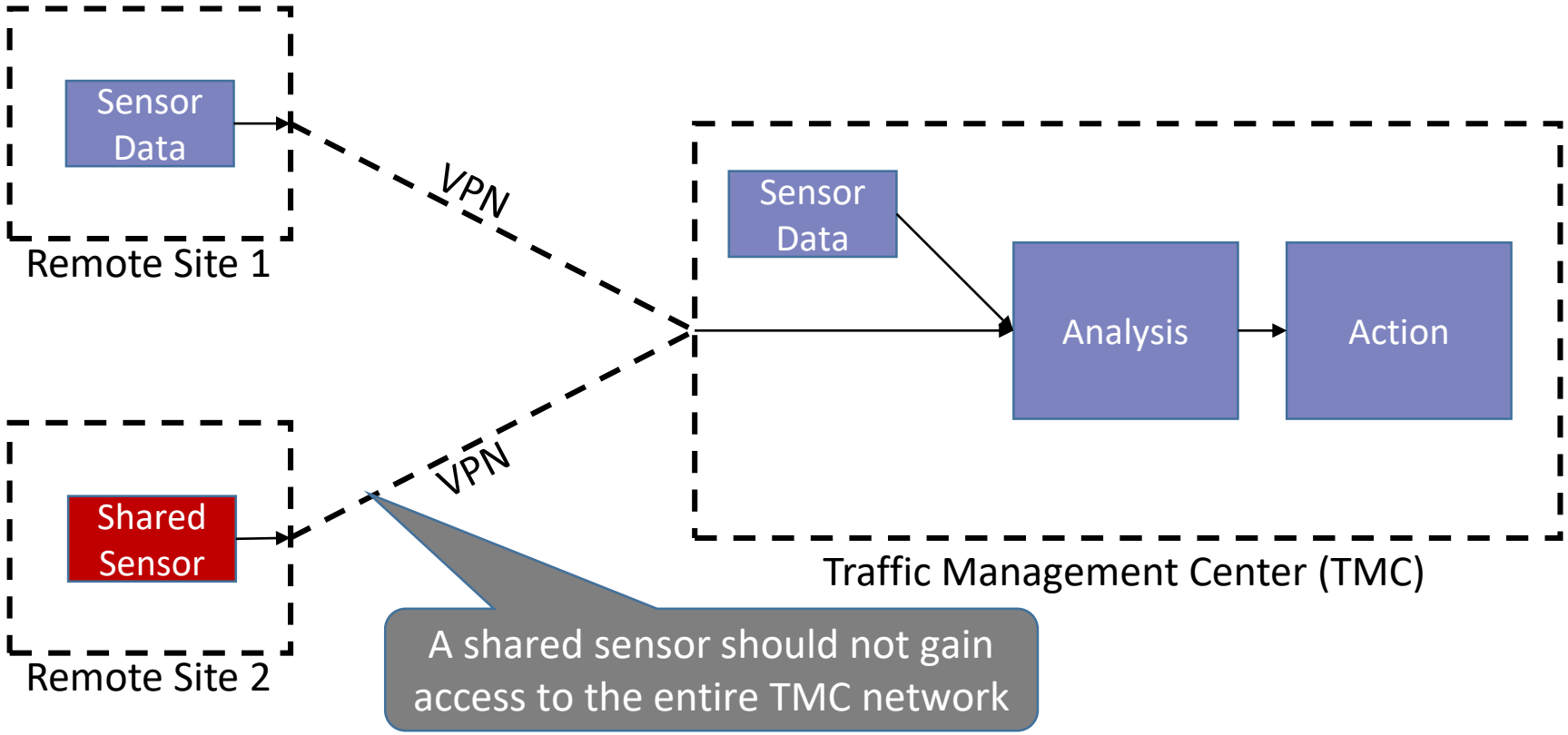


Shared Sensors and Cross Domain Data

Networks and data are not the same thing

escrypt
SECURITY. TRUST. SUCCESS.

- Applications that accept data from a shared sensor should not need to trust the entire remote network

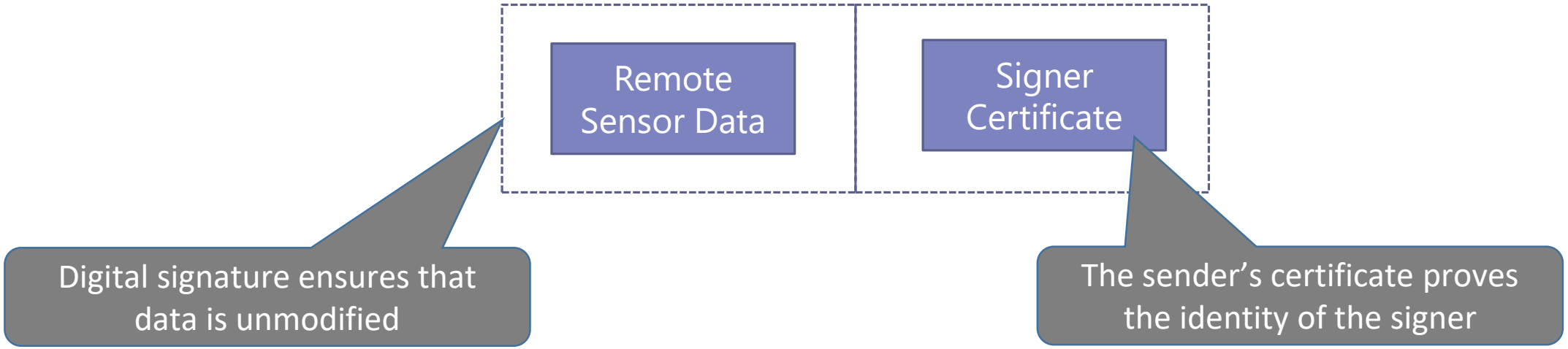


Public Key Infrastructure (PKI) and Trusted Data

Digital signatures allow for individual data elements to be validated

escrypt
SECURITY. TRUST. SUCCESS.

- A digital signature ensures the integrity of new data
- A certificate validates the identity of the data source and can optionally prove additional properties about the source
- Digitally signed data can be independently validated by multiple recipients

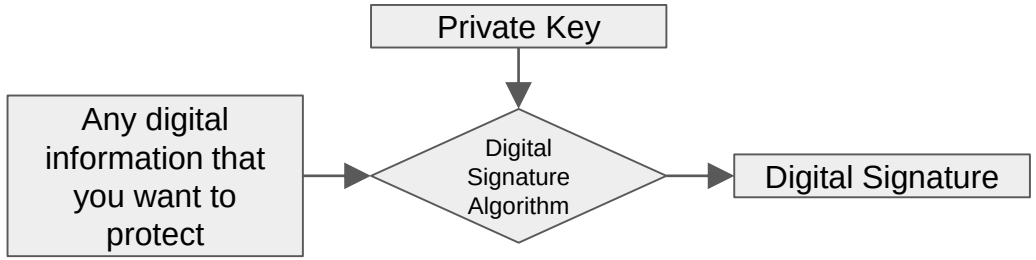


Public Key Infrastructure (PKI) and Trusted Data

PKI technology review

escrypt
SECURITY. TRUST. SUCCESS.

- PKI is a technical solution for managing trust
- The technology depends on digital “signatures”
- Signatures are created using a device’s “private” key
- Signatures are validated using a device’s “public” key

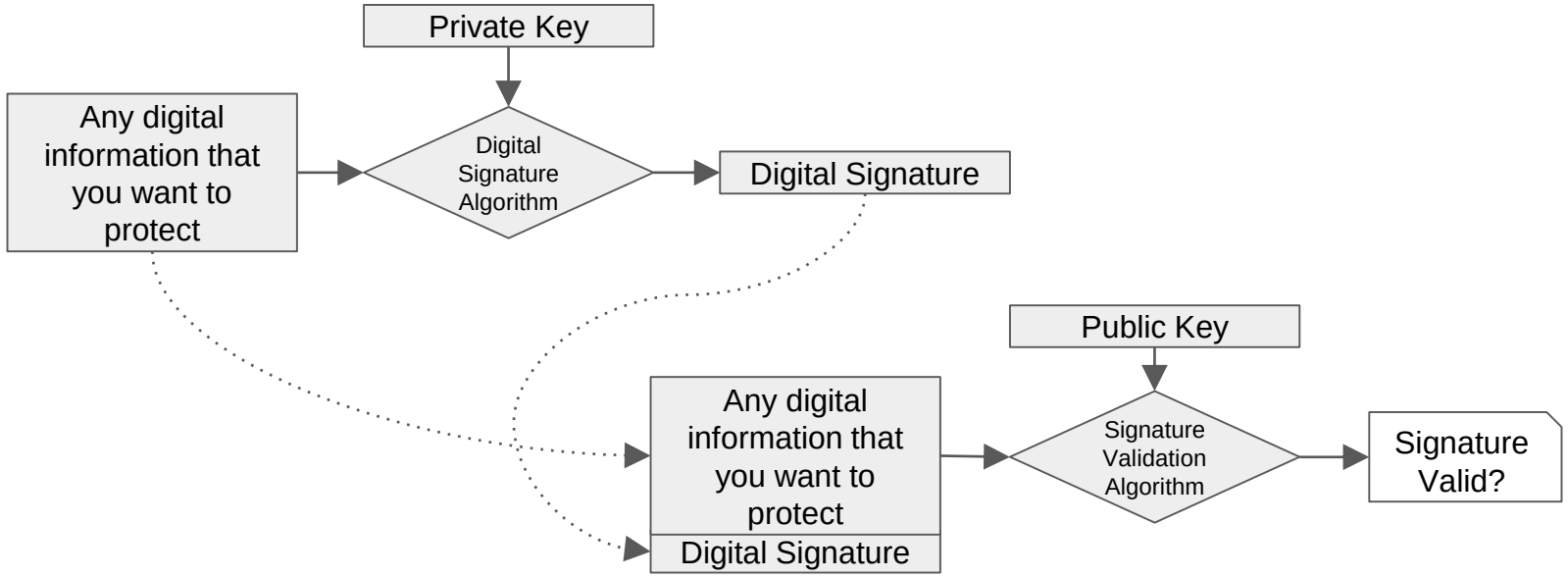


Public Key Infrastructure (PKI) and Trusted Data

PKI technology review

escrypt
SECURITY. TRUST. SUCCESS.

- PKI is a technical solution for managing trust
- The technology depends on digital “signatures”
- Signatures are created using a device’s “private” key
- Signatures are validated using a device’s “public” key

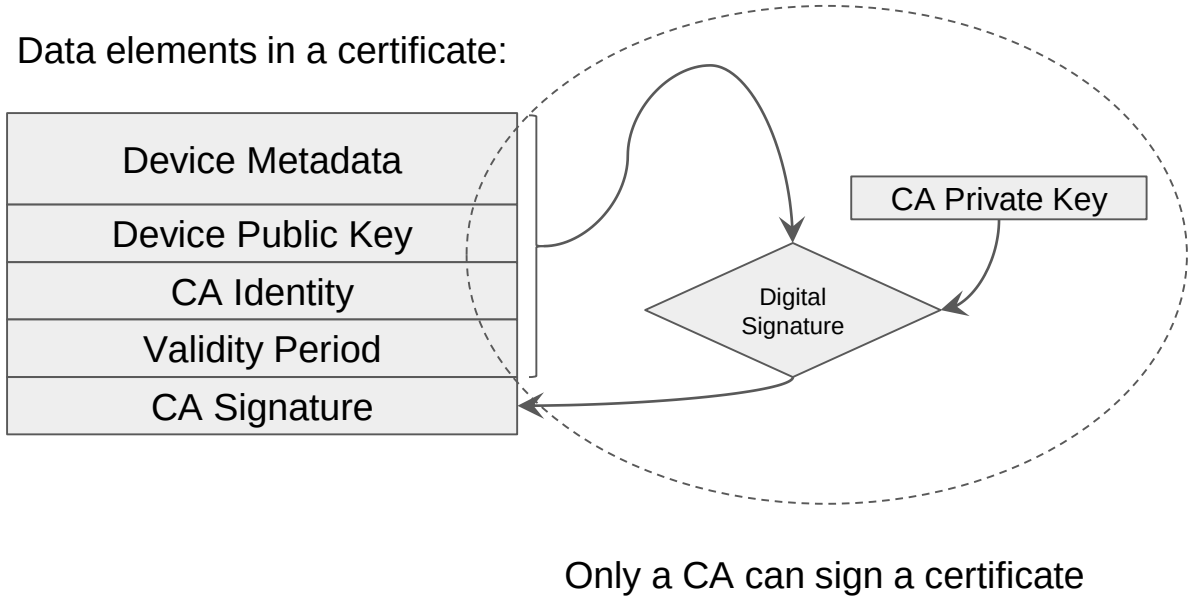


Public Key Infrastructure (PKI) and Trusted Data

PKI technology review

escrypt
SECURITY. TRUST. SUCCESS.

- A Certificate Authority (CA) is a device that can sign “certificates” using its private key
- A certificate can authorize other devices to use their own private key to sign other messages
- The certificate for a device contains the device public key and the identity of the device

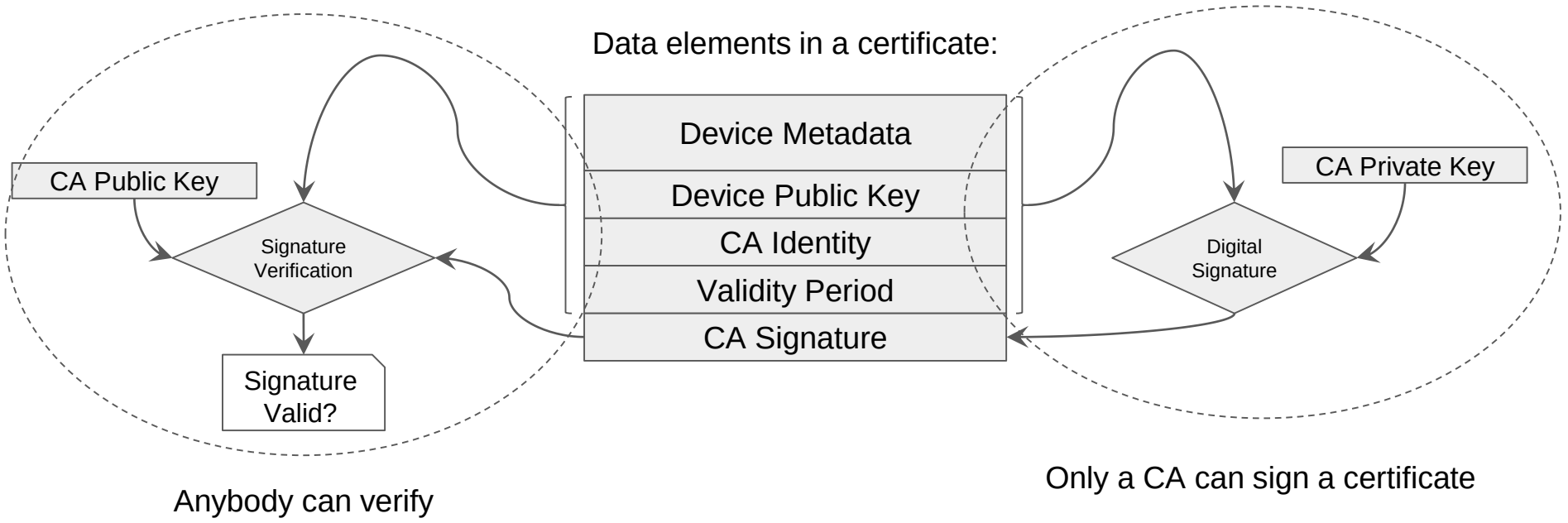


Public Key Infrastructure (PKI) and Trusted Data

PKI technology review

escrypt
SECURITY. TRUST. SUCCESS.

- A Certificate Authority (CA) is a device that can sign "certificates" using its private key
- A certificate can authorize other devices to use their own private key to sign other messages
- The certificate for a device contains the device public key and the identity of the device

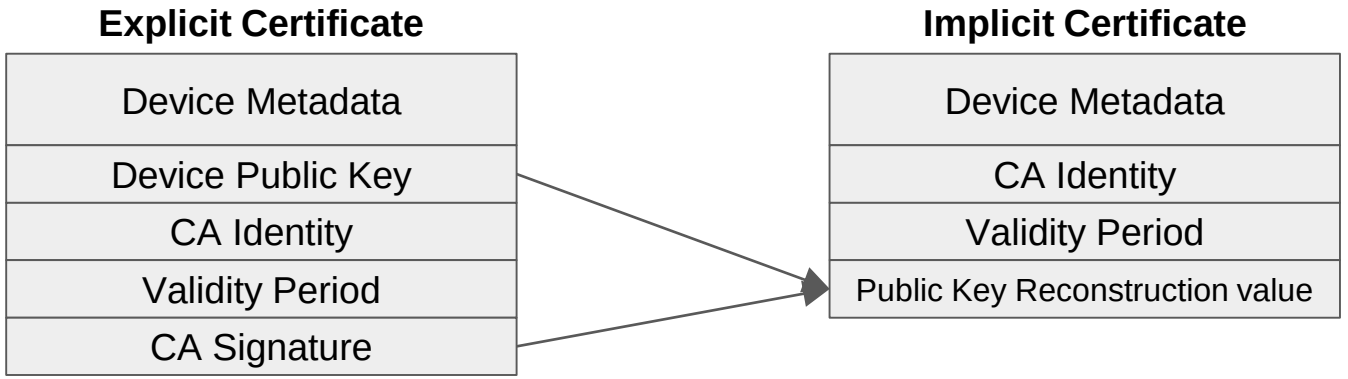


Public Key Infrastructure (PKI) and Trusted Data

PKI technology review

escrypt
SECURITY. TRUST. SUCCESS.

- Elliptic Curve Cryptography (ECC) allows for small certificates and efficient operation on embedded processors
- ECC also allows for a highly efficient certificate type called an **implicit certificate**
  - This reduces the size of every certificate by 32 bytes when used with a 256-bit elliptic curve



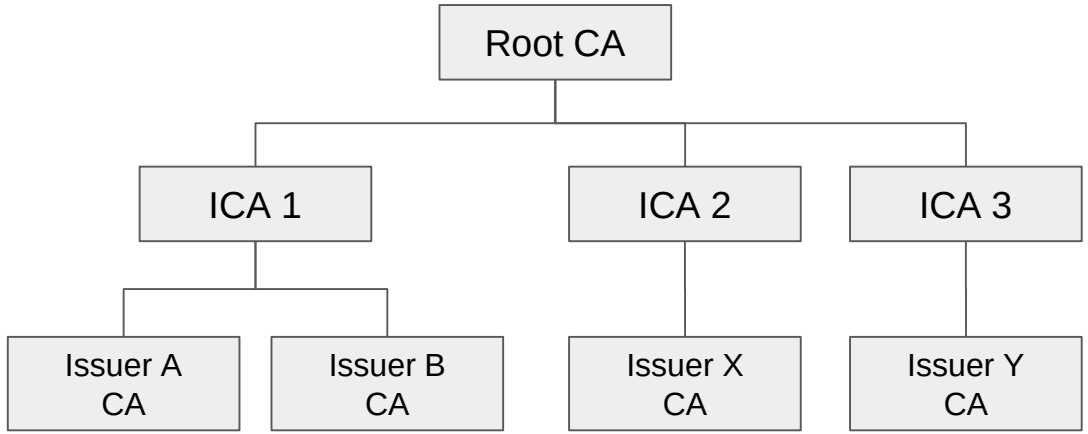
- With one operation, the recipient can reconstruct the public key and validate the CA signature on the certificate data

Public Key Infrastructure (PKI) and Trusted Data

PKI technology review

escrypt
SECURITY. TRUST. SUCCESS.

- A Certificate Authority can authorize other devices to issue certificates
- A Root CA can authorize Intermediary CAs (ICAs) to issue special-purpose certificates
- A CA lower in the hierarchy can inherit rights from the layer above, but can not add new rights

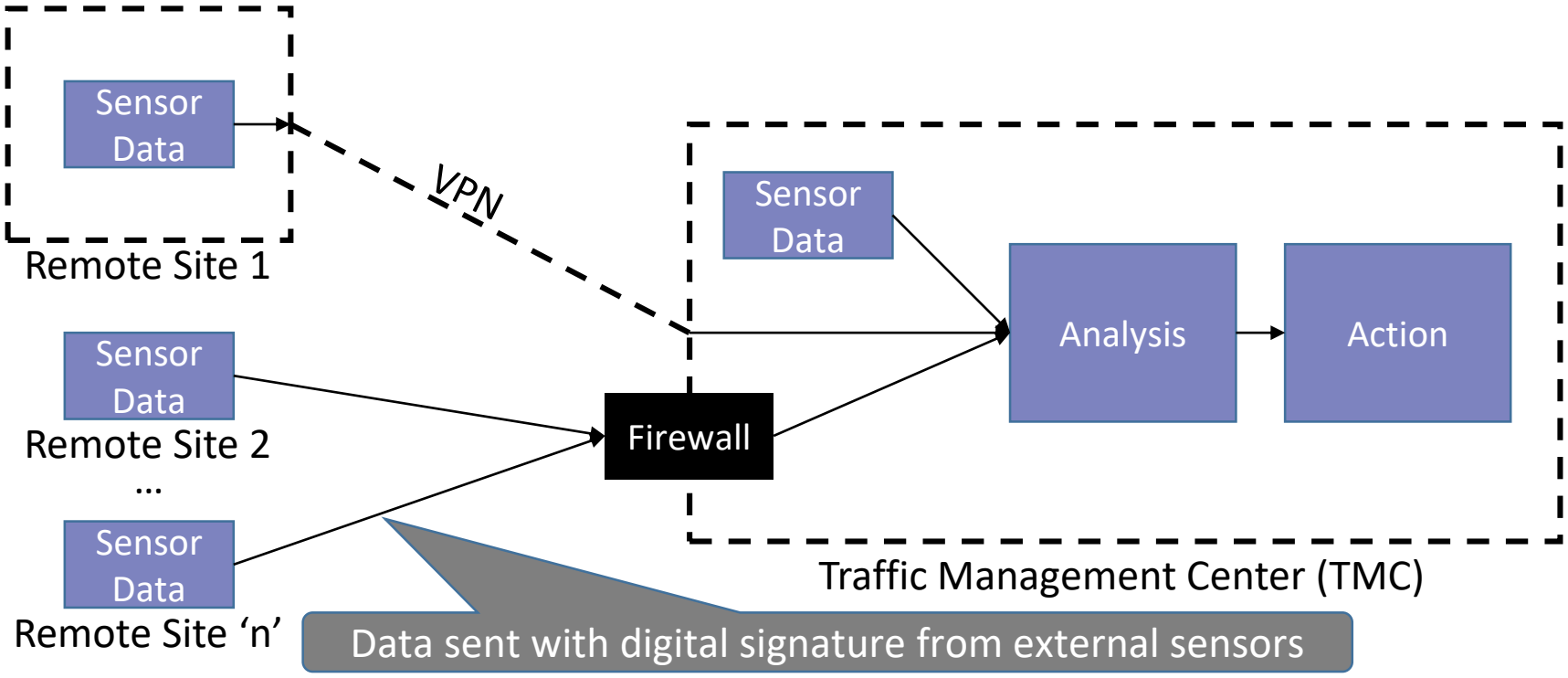


Public Key Infrastructure (PKI) and Trusted Data

Signed data can be sent over any available network

escrypt
SECURITY. TRUST. SUCCESS.

- Signed data can be accepted into a trusted network
  - The signature can be validated at the perimeter or at the application level
  - A new or unknown sender can be trusted based on trust in the authority that issued the device certificate



Smart City Complexity

Complexity is inevitable, design for it at the start

escrypt
SECURITY. TRUST. SUCCESS.

- Complex, heterogeneous systems are inevitable in city infrastructure
  - Even if you can start with a consistent architecture, future sensors and applications will demand support for new services
- PKI is designed to handle complexity
  - Independence of CAs from system operators enables new and emergent trust relationships
- Most platforms support standard X.509 certificate management today
  - Future platforms will enable more efficient standards such as implicit M2M certificates

info@escrypt.com

ESCRYPT Canada
419 Phillip Street
Waterloo, ON
N2L 3X2
Canada

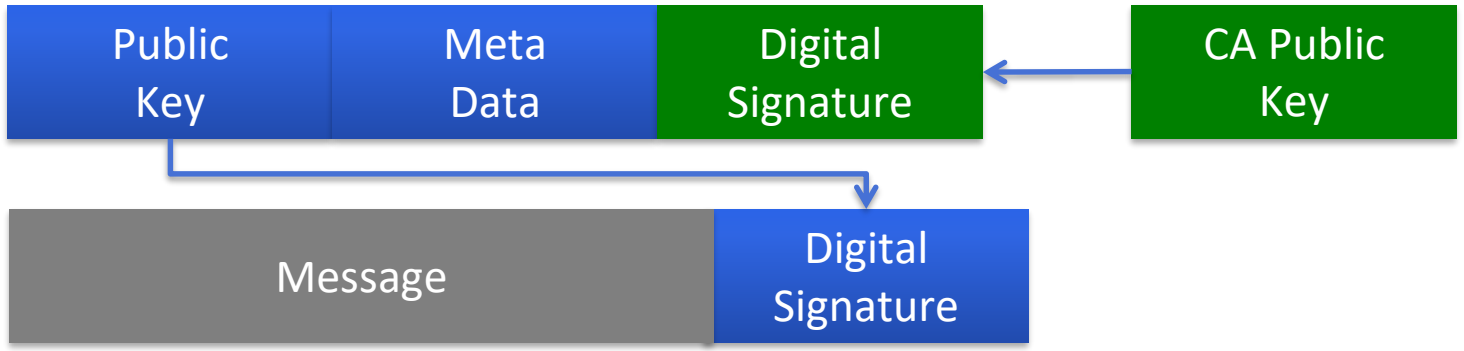
info@escrypt.com
www.escrypt.com

Backup Slides

Implicit Certificate Details

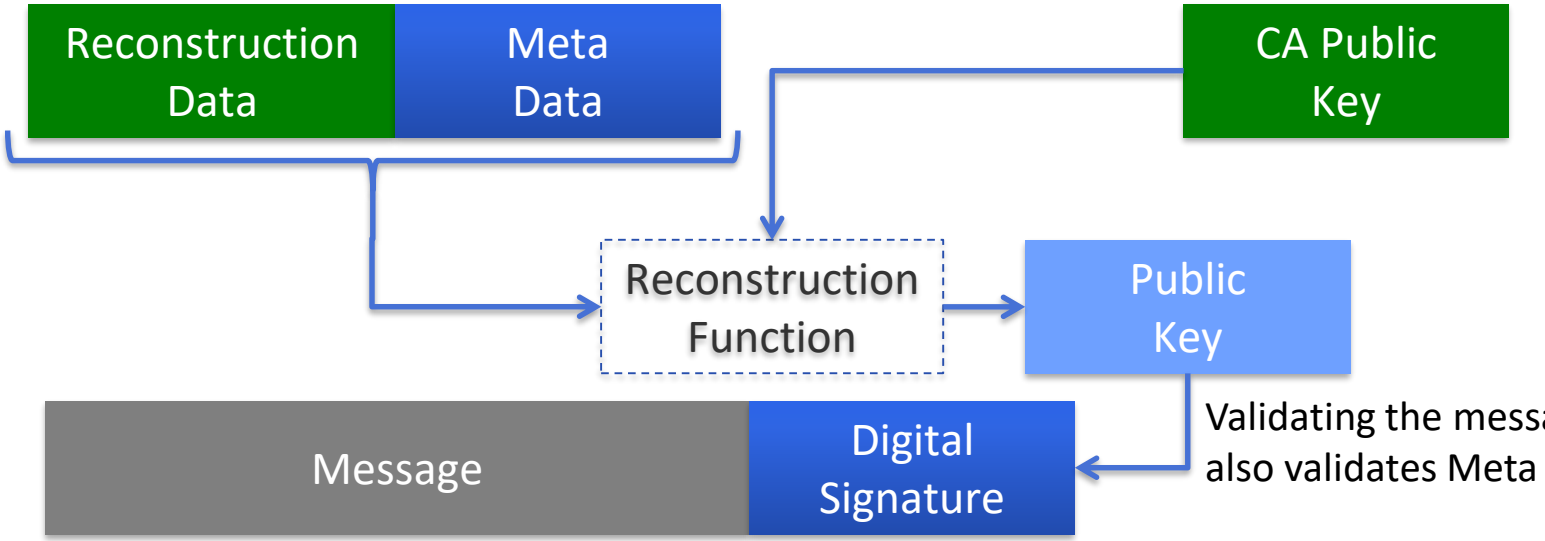
escrypt
SECURITY. TRUST. SUCCESS.

Typical digital certificate has 3 parts: ~150 Bytes



User must know:

Implicit certificate is much smaller: ~90 Bytes



Full details at: https://en.wikipedia.org/wiki/Implicit_certificate

Physical Security Requirements

All security components require FIPS 140-2 Level 3

escrypt
SECURITY. TRUST. SUCCESS.

- The Federal Information Processing Standard (FIPS) document number 140-2 is a standard that devices physical security and access control.
  - It defines 4 levels of physical security
- Currently, all SCMS back-end components must be compliant with FIPS 140-2 Level 3 security requirements
  - Level 3 requires strong “tamper resistance”
  - “compliant” is not the same as “certified”, may require less testing
  - Most V2X chipsets from leading vendors will meet this requirement

Inherent Tension

It is difficult to prove authenticity while also supporting privacy

escrypt
SECURITY. TRUST. SUCCESS.

Authenticity

Need to validate that messages are from trusted devices

- Prevent attackers from creating fake messages to change traffic patterns or create a road hazard

VS.

Privacy

Can't make it easy to track personal cars

- Each BSM contains exact position information
- Data is sent unencrypted to enable fast response time

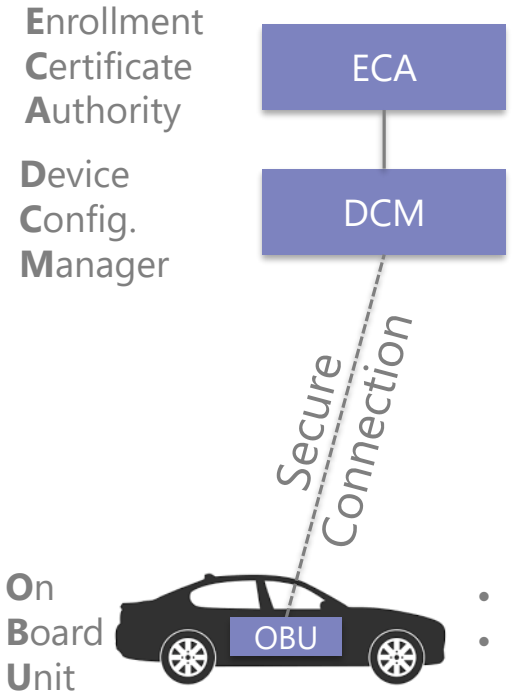
- Digital Signatures can prove that a message is "authentic" and unmodified, but only if you know you can trust the sender
- How do you trust the sender if you can't know who the sender is?

Enrolment Process

Each vehicle must be enrolled during manufacturing

escrypt
SECURITY. TRUST. SUCCESS.

- A new OBU must be enrolled before it can participate in the SCMS
- An enrollment certificate acts as a trusted "ticket", used for accessing SCMS services and downloading files



- ECA issues enrollment certificates
- Every enrollment certificate is assigned to a specific RA
- ECA trusts that messages sent through the DCM came from a real OBU

- DCM needs to confirm that it is connected to a real OBU
- May perform software updates or integrity checks
- Installs a Local Certificate Chain File (LCCF) which includes a copy of the Root CA(s)
- Installs a Local Policy File (LPF) which defines security-critical policies

- An OBU can be enrolled before or after installation in a vehicle
- Recommended that each OBU generates it's own private key for enrollment (but secure key injection is allowed)