Vehicle to Vehicle Safety Application using ECC PKI

NIST Workshop on Elliptic Curve Cryptography Standards

June 11, 2015

TRUSTPOINT
INNOVATION TECHNOLOGIES, LTD.

V2V Significance

Safety

33,561 highway deaths in 2012
5,615,000 crashes in 2012
Leading cause of death for ages 4-27

Mobility

5.5 billion hours of travel delay
$121 billion cost of urban congestion

Environment

2.9 billion gallons of wasted fuel
56 billion lbs. of additional CO_2

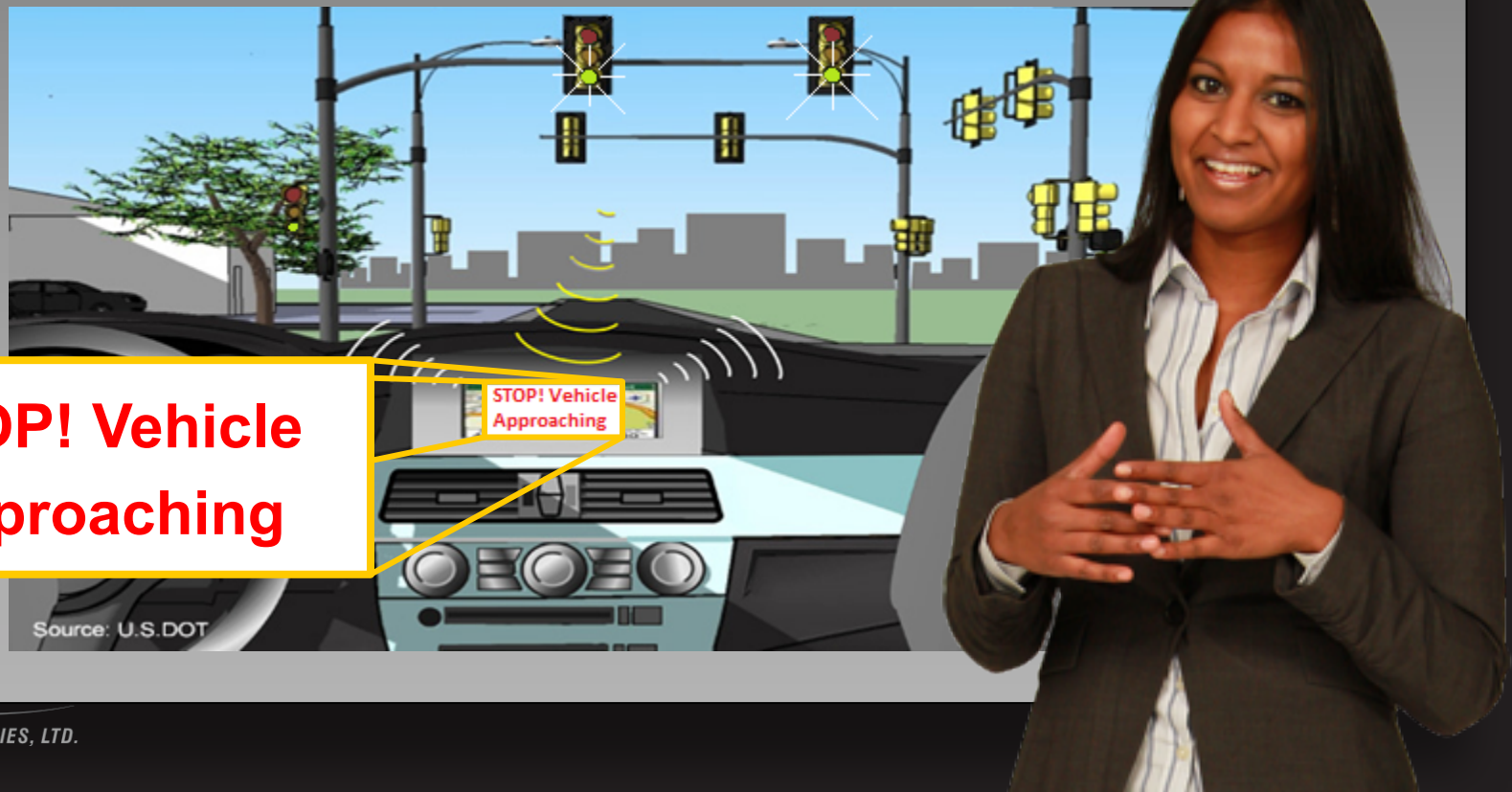
TRUSTPOINT
INNOVATION TECHNOLOGIES, LTD.

V2X Capabilities

- V2X has the potential to avoid 80% of crashes involving unimpaired drivers
- Greater situational awareness:
  - Your vehicle can “see” nearby vehicles and knows roadway conditions you cannot see
  - 360-degree “visibility”
- Reduce or even eliminate crashes through:
  - Driver advisories
  - Driver warnings
  - Vehicle control

Safety Applications: V2V Scenario

Lauren is driving home with her son after school. She is stopped at a red light. When the light turns green, she is about to move through the intersection when she is warned of a vehicle crossing the path in front of her. She quickly brakes to avoid a T-bone crash.



STOP! Vehicle Approaching

V2X Capabilities

- V2V effectiveness increases with *deployment saturation*
- V2I can improve initial performance:
  - e.g. Stoplights can use sensors to detect oncoming vehicles and warn V2I equipped drivers of oncoming vehicles likely to run through a red light.
- V2V's PKI is in a Proof Of Concept (POC) phase

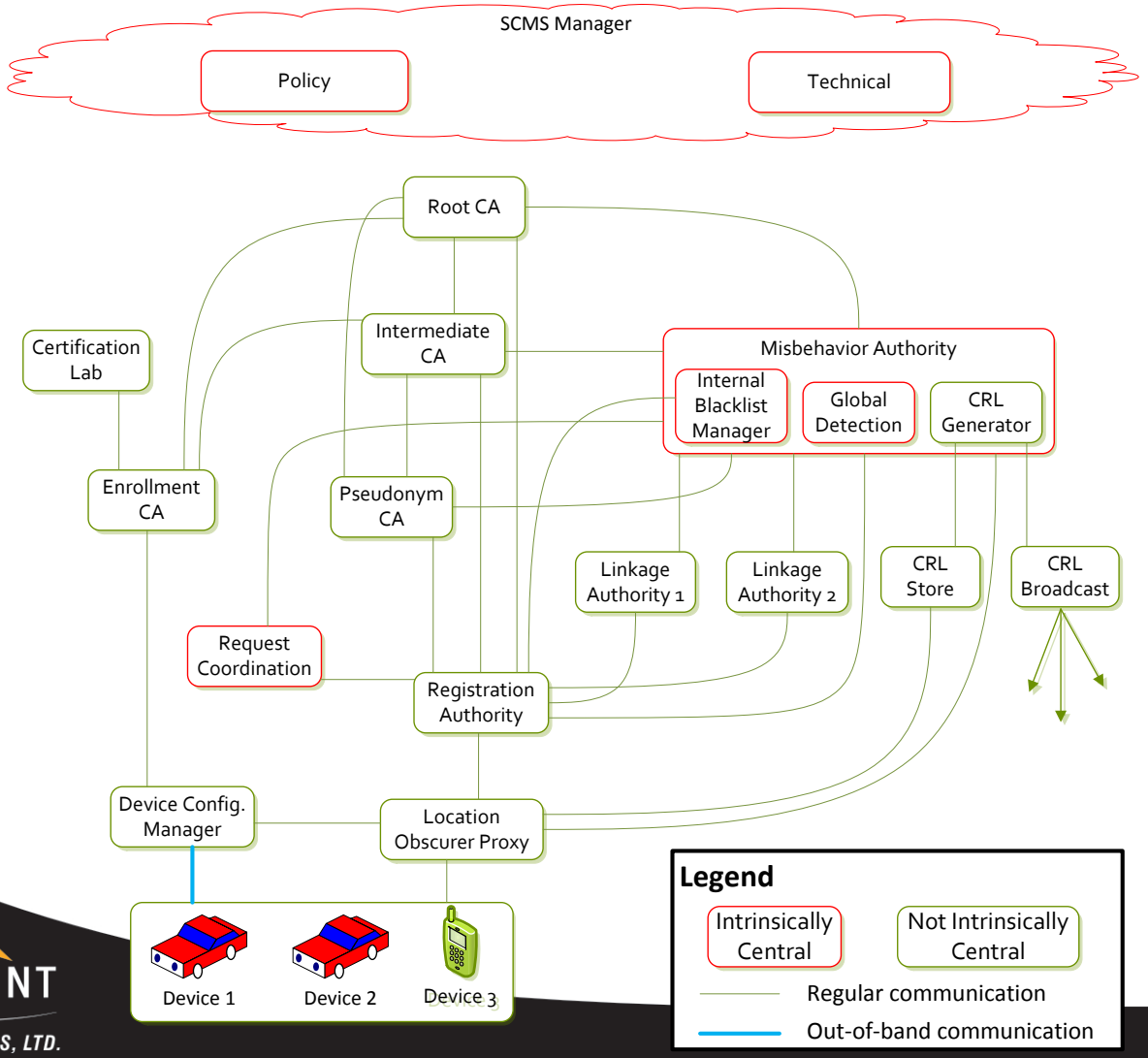
Complex Security Design

- System mandates:
  - Privacy for users: No Personal Ident Information (PII)
  - Prevent tracking by insiders & outsiders
  - Assume errors and hackers
  - Detect and remove misbehaving systems
  - Minimize over the air messaging bandwidth
- Tricky to Achieve:
  - Need high volume of small anonymous short lived certificates
  - … and still be able to revoke the certs when needed

ECC PKI Required

- Challenging embedded environment
  - 10x messages per vehicle per second
  - Up to 300 vehicles in range
  - memory and limited bandwidth
  - Each vehicle provisioned with 1000s of certs
  - Some vehicles may be offline for long periods
- Large Volume of Certificates
  - 45,000 x the largest CA to date (full deployment)
  - Volume driven by short-lived certificate design

V2X PKI Architecture



TRUSTPOINT
INNOVATION TECHNOLOGIES, LTD.

System Parameters

- Standards
  - NIST P-256 curve
  - ECDSA (FIPS 186-3)
  - ECIES (IEEE 1363a)
  - SHA-256 (FIPS 180-3)
  - AES-CCM (NIST SP 800-38C)
  - IEEE 1609.2 messaging (ASN.1)
- Interesting Exceptions
  - ECQV (*SEC4, no NIST standard yet)
  - Butterfly key expansion (*unique to V2V, no standard)

Stylized ECQV

U		CA
$k_U \in_R [1, n)$		
$R_U := k_U G$	$\xrightarrow{U, R_U}$	
		$k \in_R [1, n)$
		$P_U := R_U + kG$
		$Cert_U := Encode(P_U, U, *)$
		$e := H_n(Cert_U)$
		$r := ek + d_{CA} \bmod n$
$e := H_n(Cert_U)$	$\xleftarrow{r, Cert_U}$	
$d_U := ek_U + r \bmod n$		

TRUSTPOINT
INNOVATION TECHNOLOGIES, LTD.

Hash for ECQV

$H_n : \{0, 1, \ldots, 255\}^* \to [0, n)$
maps octet strings to integers modulo n.

Input:

1. An arbitrary length octet string S.
2. H hash function output length *hashlen*.
3. An integer n.

Actions:

1. Compute $h = H(S)$ (*hashlen* bits).
2. Set e to leftmost $\lfloor \log_2 n \rfloor$ bits of h.

Output: Integer e in $[0, n)$.

TRUSTPOINT
INNOVATION TECHNOLOGIES, LTD.

Private/Public Correspondence

$$
\begin{aligned}
d_U &= ek_U + r \pmod{n} \\
&= ek_U + ek + d_{CA} \pmod{n}
\end{aligned}
$$

$$
\begin{aligned}
Q_U &= eP_U + Q_{CA} \\
&= e(R_U + kG) + Q_{CA} \\
&= e(k_U G + kG) + d_{CA} G \\
&= (ek_U + ek + d_{CA})G
\end{aligned}
$$

TRUSTPOINT
INNOVATION TECHNOLOGIES, LTD.

Reconstruction

Private:

$$d_U := ek_U + r \bmod n$$

Public:

$$e := H_n(Cert_U)$$
$$Q_U := eP_U + Q_{CA}$$

Here Q_{CA} a system parameter, similar to curve.

TRUSTPOINT
INNOVATION TECHNOLOGIES, LTD.

Pros/Cons

Certificate components:

- ECDSA: P, r, s: $3 + \epsilon$ finite field elements.
- ECQV: P_U: $1 + \epsilon$ finite field elements.

This size difference is crucial in V2V, where many messages must traverse a low bandwidth channel.

However, we now must delay our assurance until the private key has been *used*.

TRUSTPOINT
INNOVATION TECHNOLOGIES, LTD.

Butterfly Expansion (William Whyte)

Certificate components:

- Base point: $R_U = k_U G$.
- Keyed Index: $f_K(i)$ keyed indexed function producing an EC private key.
- Expansion: $R_{U,i} = R_U + f_K(i)G$.

Expansion at the RA produces multiple public keys from one request.
Request value R_U is expanded to $R_{U,i}$
Each $R_{U,i}$ processed by the CA as R_U before.

TrustPoint
INNOVATION TECHNOLOGIES, LTD.

Butterfly Expansion (William Whyte)

- V2V-unique feature for certificate requests
  - Each vehicle requests 3000 certs initially (1000 annual)
  - Desire to reduce the volume of requests on the uplink
- Butterfly expansion actors
  - Client sends one public key and a keyed expansion function
  - RA expands the public keys into a series
  - RA shuffles requests from multiple clients
  - CA contributes to the client private key series
  - CA generates certs for derived public keys
  - CA encrypts certificates to client (privacy)
  - Client generates matching private keys.

Anonymous Revocation

- Critical to privacy and robustness
  - Vehicles change certificates frequently
  - Certificates do not contain identifying information
  - Yet, all of a vehicle's current and future certificates can be revoked by placing information on the CRL
  - Revocation destroys privacy for vehicle, but only forward in time, not backward

Linkage Values

- Anonymous revocation achieved with a pair of hash chains, seeded uniquely to a vehicle (Linkage Authorities)
- XOR of hash chain values used as cert pseudonym
- Hash chains advance at a defined system rate
  - All vehicles re-compute current revoked pseudonyms at each new time period
  - CRL's are periodically updated to current time periods
- Linkage Authorities operated separately for security and privacy protection

Relevance to NIST

- The largest PKI ever deployed will be ECC based
- Butterfly key expansion, Linkage Authorities
- The ECQV algorithm would benefit from NIST certification/compliance testing
- US Gov funded project, using US Gov curves for the POC, would like to know NIST's intentions for future curves to prepare for deployment