Privacy-Enhanced Capabilities for VANETs using Direct Anonymous Attestation

Jorden Whitefield

Aalto University, 17^{th} September 2018

Surrey Centre for Cyber Security
Department of Computer Science
University of Surrey
sccs.surrey.ac.uk

Outline

- Security & Privacy challenges of Intelligent Transportation Systems
- Trusted Computing for Automotive
- Application of DAA within VANETs
- Implementation
- Future Research

ITS Security & Privacy Challenges

Contradictory positions between users and infrastructure entities. . .

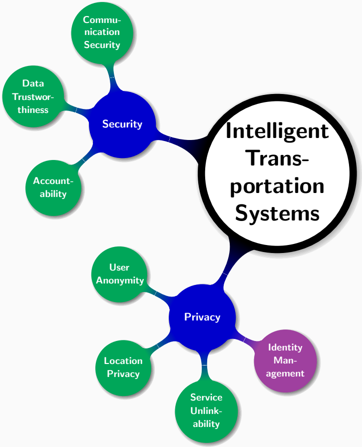
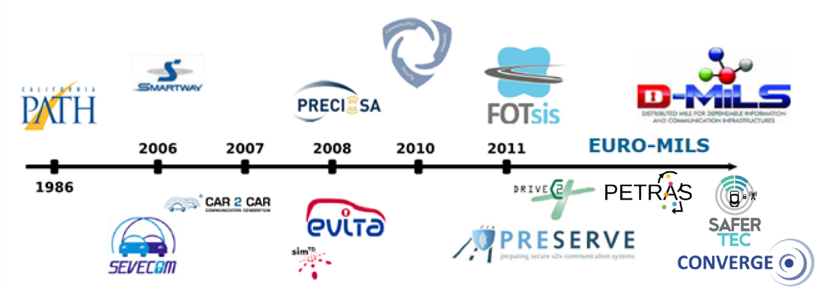


Image source: "Trustworthy People-Centric Sensing: Privacy, Security and User Incentives Road-Map"

- Protect the Users from the System (i.e., user privacy)
  - ⇒ Anonymity (conditional)
  - ⇒ Pseudonymity
  - ⇒ Unlinkability
  - ⇒ Unobservability
- Protect the System from the Users (i.e., trustworthiness)
  - ⇒ Authentication & Authorization
  - ⇒ Accountability
  - ⇒ Data Trustworthiness

Security & Privacy Architectures - Close to deployment

- Many standardization bodies
  - ✓ Car 2 Car Communication Consortium (C2C-CC)
  - ✓ IEEE & ETSI standard specifications



But safety is the key pillar

- Vehicular Communications (VC)
- Vehicles propagate information for Safe-Driving
  - Location, Velocity, angle
  - Hazardous warnings
  - Emergency break etc.
- Cooperative awareness through beaconed status messages and event-triggered warnings
- . . . Security in VC?
  - Assure legitimate vehicles propagate information
  - Secure integrity of information

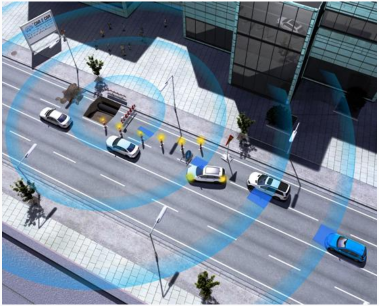


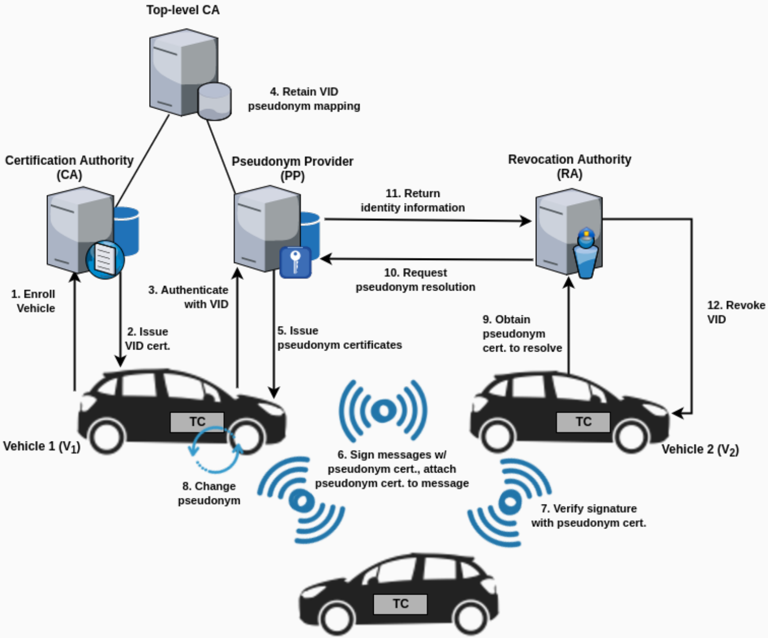
Image source: Car-2-Car Consortium

The Challenge

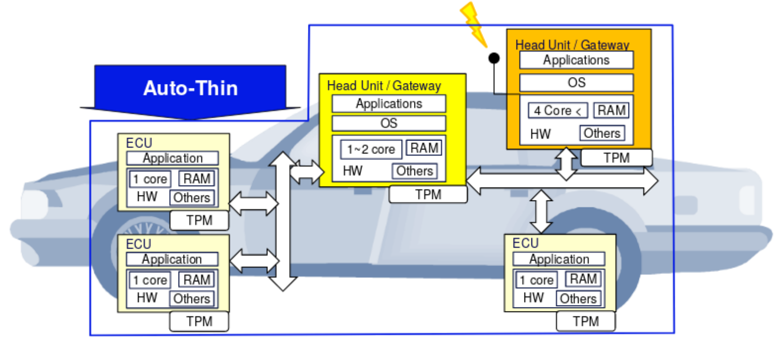
Deploy an ITS with security & privacy built-in, which is scalable providing vehicles with

- Protection from **trusted** & **colluding** third parties
- **Privacy** and **unlinkability**, while still being held **accountable**
- Scalable and dependable **authentication, authorization** & **revocation**
- Solutions that abide by the **VC standards**

State-of-the-art VPKI



Trusted Computing for Automotive



- Trusted Platform Module (TPM) provides:
  - ⇒ Isolation
  - ⇒ Protected Execution
  - ⇒ Shielded Storage
- Secure crypto processor: creates, stores, uses crypto keys
- TCG developing TPM for "Automotive Thin Profile"[1]

[1] https://trustedcomputinggroup.org/wp-content/uploads/TCG_TPM_2.0_Automotive_Thin_Profile_v1.1-r15.pdf

Direct Anonymous Attestation

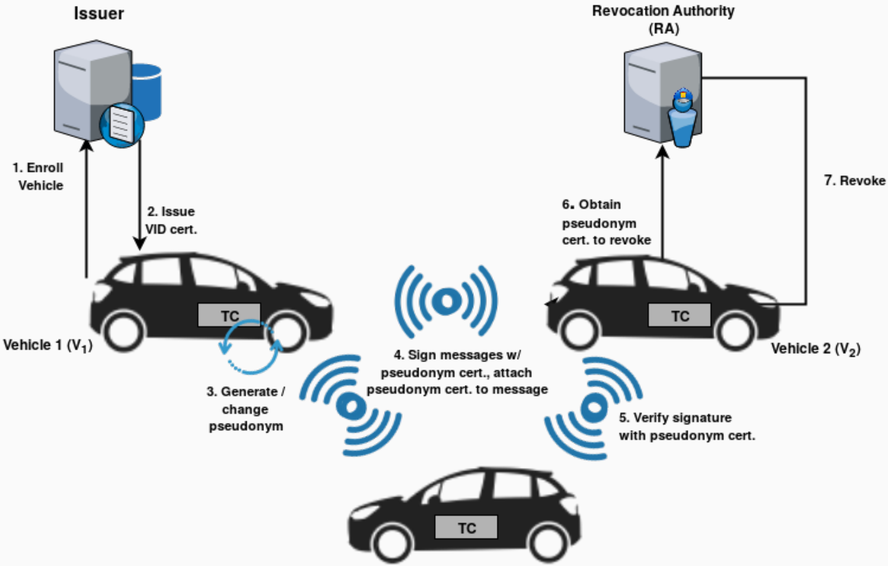
- Anonymous digital signature scheme
  - $\Rightarrow$ Strong, but privacy preserving authentication.
- Hardware-based attestation using TPMs
- Properties of DAA include:
  - $\Rightarrow$ **Correctness:**
    - $\rightarrow$ Valid signatures only producible by honest platforms, and are verifiable and linkable when specified.
  - $\Rightarrow$ **User-controlled Anonymity:**
    - $\rightarrow$ Identity of user cannot be revealed.
  - $\Rightarrow$ **User-controlled Traceability:**
    - $\rightarrow$ The host controls whether signatures can be linked.
  - $\Rightarrow$ **Non-Frameability:**
    - $\rightarrow$ Adversary should not be able to impersonate honest platforms.
- Standardised in ISO/IEC 20008-2 & 11889

DAA Pseudonym Scheme - Overview

- Simplified VPKI Architecture
  - ⇒ **Issuer:** Authenticates vehicles' to ITS and issues DAA credential
  - ⇒ **Revocation Authority:** Removes misbehaving / malfunctioning vehicles'
- Decentralised ITS allows a shift-of-trust into vehicles.
  - ⇒ Vehicles responsible for self-signing pseudonyms
  - ⇒ Promotes scalability - *Certificate Revocation Lists* not required
- Timely and "*in the moment*" revocation
- Vehicles in control of privacy
- Utilises trusted hardware and uses DAA for hardware-based attestation

Trusted third parties gain no knowledge of ITS entities from colluding with one another.

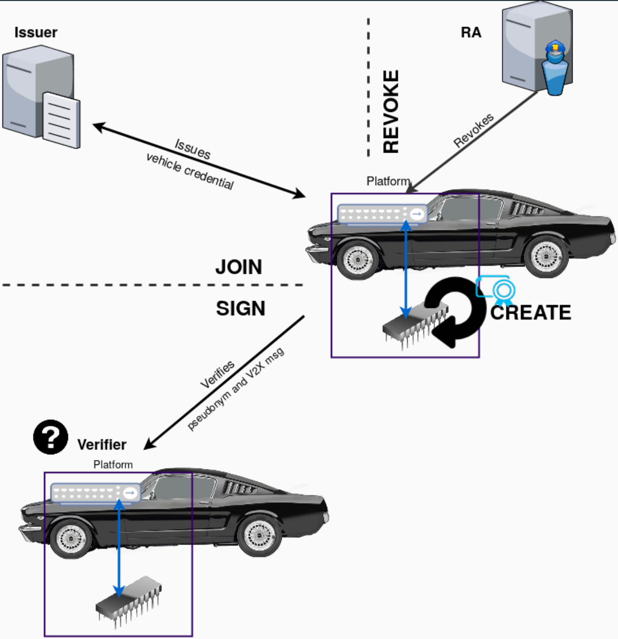
DAA Pseudonym Scheme - Architecture



DAA Protocols for VANETs

- SETUP: TC generates fresh DAA key-pair from Issuers security parameters.
- JOIN: Attests that a vehicle has a valid TC, and produces the DAA credential from Issuer $\Rightarrow$ authenticated member of ITS.
- CREATE: Fresh self-signed pseudonyms created by TC using credential.
- SIGN/VERIFY: Authenticated V2X communication that verifies pseudonym is valid.
- REVOKE: Verifiable revocation that a vehicle has been removed from ITS. Performed without pseudonym resolution.

DAA Protocols for VANETs



CREATE Protocol

Create: TC	$\rightleftharpoons$	HOST
sk_{tc}		cre
		`fresh` r
`fresh` sk_{ps}/pk_{ps}	$\xleftarrow{\texttt{"create"} \parallel \widehat{cre}}$	$\widehat{cre} :=$ `blind`(cre, r)
`fresh` r'		
$ps_{sig} :=$ `DAASign`$(pk_{ps}, r', sk_{tc}) = (\sigma_1 \parallel \sigma_2 \parallel \widehat{cre})$		
$\sigma_1 :=$ `sign`(pk_{ps}, sk_{tc})		
$\sigma_2 :=$ `blindSign`$(\texttt{"certified"} \parallel pk_{ps}, r', sk_{tc})$		
$ps_{Cert_{tc}} := (pk_{ps} \parallel ps_{sig})$		
`store`(sk_{ps})	$\xrightarrow{ps_{Cert_{tc}}}$	`store`$(ps_{Cert_{tc}})$

1. Credential (from JOIN) is blinded by the host for privacy
2. DAASign produces two signatures: σ_1 (*deterministic*) & σ_2
3. Pseudonym is a key-pair with a DAA signature associated with a blinded credential.

REVOKE Protocol

Revoke: TC	$\rightleftharpoons$	HOST	$\rightleftharpoons$	RA
sk_{tc}, pk_{ra}		cre		$pk_I, pk_{ps}, ps_{Cert_{tc}}, sk_{ra}$
				$msg := \{\| \texttt{"revoke"} \,\|\, pk_{ps} \,\|\, \texttt{reason} \,\|\}_{sk_{ra}}$
		$\texttt{fresh}\ r$	$\xleftarrow{msg}$	
$\texttt{verify}(msg, pk_{ra})$	$\xleftarrow{\widehat{cre}, msg}$	$\widehat{cre} = \texttt{blind}(cre, r)$		
$\texttt{fresh}\ r'$				
$\sigma_{rvk} := \texttt{DAASign}(pk_{ps}, r, sk_{tc}) = (\sigma_1^{ra} \parallel \sigma_2^{ra} \parallel \widehat{cre})$				
$\sigma_1^{ra} := \texttt{sign}(pk_{ps}, sk_{tc})$				
$\sigma_2^{ra} := \texttt{blindSign}(\texttt{"confirm"} \parallel pk_{ps}, r', sk_{tc})$	$\xrightarrow{\sigma_{rvk}}$	σ_{rvk}	$\xrightarrow{\sigma_{rvk}}$	$\texttt{eq}(\sigma_1, \sigma_1^{ra}, \texttt{true})$
				$\texttt{DAAVerify}(\sigma_{rvk}, pk_I)$

1. Vehicle receives revocation message from RA, and TC verifies authenticity.
2. TC creates DAA signature to check if σ_1^{ra} matches σ_1
3. If match create revocation confirmation and delete all pseudonyms & DAA key-pair

Security Model

- Security & Privacy Analysis
  - ⇒ User-controlled Anonymity and Traceability:
    - → Pseudonym creation DAA credential blinded, not linkable to vehicle.
    - → DAA credential does not contain any PII.
  - ⇒ Non-frameability:
    - → Communication from vehicle cannot be faked or generated by adversary.
    - → SIGN / VERIFY message is signed by TC, assured by the DAA credential of pseudonym.
  - ⇒ Assurance of revocation:
    - → Revocation requests and confirmations verified by both RA and vehicle.
    - → Confirmed revocation executes deletion of all pseudonyms and DAA credentials.

Research Directions

- Implementation and Experimentation
  - ⇒ Message / signature sizes
  - ⇒ Timings for signature verification
  - ⇒ Host or TC: "Trusted VS Untrusted"
- Formal Analysis using the Tamarin Prover
  - ⇒ Verify trace properties, e.g., security / authentication
  - ⇒ Analysis of V2X revocation[2]
  - ⇒ Develop theory for proving DAA in symbolic setting (General theory useful beyond vehicular use case)
- Revocation correctness
  - ⇒ How revocation messages reach the host?
  - ⇒ Message Indistinguishability, Heartbeat?

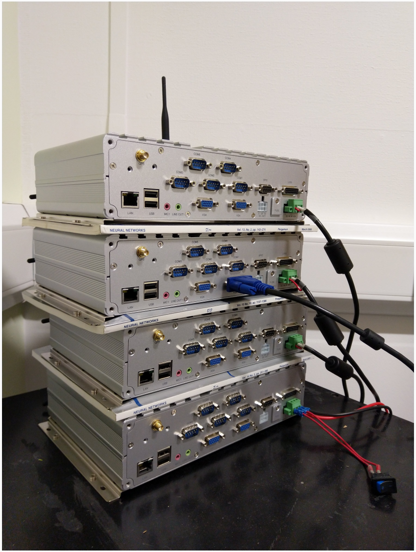
[2] "**Formal Analysis of V2X Revocation Protocols**" by Whitefield et al. STM 2017, Oslo, Norway

EPSRC UK Impact Accelaration Account

- Demonstrate the applicability of our DAA V2X architecture:
  - ⇒ Implemented in a relevant lab environment using actual automotive boxes and TPMs.
  - ⇒ Communication interfaces.
  - ⇒ DAA scheme compliant with ISO/IEC 20008-2 and 11889
- Project in collaboration with:
  - ⇒ Thales Research and Technology UK.
  - ⇒ Thales eSecurity.
  - ⇒ Pervasive Intelligence.
  - ⇒ University of Surrey.

Implementation: Hardware

- Nexcom VTC 6200
  - ⇒ Intel Atom D510 Dual Core 1.6GHz
  - ⇒ 2GB RAM
  - ⇒ Internal wireless communication (3.5G, GSM/GPRS, WLAN, BT)
  - ⇒ Voyage Linux (Lightweight Debian)



Implementation: Hardware

When Cryptography meets the real world

Join Protocol I of IV

The Join Operation

TPM		Host		Issuer
		$(X,\ Y) \in \mathbb{G}_2 \times \mathbb{G}_2$		$(x,\ y) \in \mathbb{Z}_n \times \mathbb{Z}_n$
INITIALISE				
generate and store $(e, \mathcal{E})$				
choose and store $f \in \mathbb{Z}_n$				
$Q_2 = [f]P_1$				
GET_ENDORSEMENT_KEY_DATA				
send $\mathcal{E}$PD to Issuer	$\xrightarrow{\mathcal{E}\text{PD}}$	extract and store $\mathcal{E}$	$\xrightarrow{\mathcal{E}\text{PD}}$	extract and check $\mathcal{E}$
GET_DAA_KEY_DATA				
send Q_2PD to Issuer	$\xrightarrow{Q_2\text{PD}}$	extract and store Q_2	$\xrightarrow{Q_2\text{PD}}$	check Q_2PD
				store Q_2PD
				$\mathcal{K}_1 \leftarrow \{0,1\}^t$
				store $\mathcal{K}_1$
				$s_1 \leftarrow \{0,1\}^t$

Join Protocol II of IV

TPM		Host		Issuer
		$(X,\ Y) \in \mathbb{G}_2 \times \mathbb{G}_2$		$(x,\ y) \in \mathbb{Z}_n \times \mathbb{Z}_n$
ACTIVATE_CREDENTIAL				
	$\xleftarrow{\text{CB}_1,\ \hat{s}_1}$	- - - - - - - -	$\xleftarrow{\text{CB}_1,\ \hat{s}_1}$	generate CB_1 and $\hat{s}_1$
$\mathcal{K}_1 = \text{activate credential}(\text{CB}_1, \hat{s}_1)$	$\xrightarrow{\mathcal{K}_1}$	$str = X \parallel Y \parallel \mathcal{K}_1 \parallel \mathcal{E}$		
INITIATE_DAA_VALIDATION				
calculate a counter value cv				
$u_{cv} \leftarrow \mathbb{Z}_n$				
$U = [u_{cv}]P_1$	$\xrightarrow{U, cv}$	store cv		
COMPLETE_DAA_SIGNATURE				
$p_{tpm} = H_{12}(p)$	$\xleftarrow{p, cv}$	$p = H_2(P_1 \parallel Q_2 \parallel U \parallel str)$		
old - - - - - - - -				
$v = p_{tpm} \pmod{n}$				
$w = u_{cv} + v \cdot f \pmod{n}$				
$\sigma_{ch} = (v, w)$				
new - - - - - - - -				
$n_J \leftarrow \{0,1\}^t$				
$v = H_5(n_J \parallel p_{tpm})$				
$w = u_{cv} + v \cdot f \pmod{n}$				
$\sigma_{ch} = (n_J, w)$	$\xrightarrow{\sigma_{ch}}$	$p_{tpm} = H_{12}(p)$		

Join Protocol III of IV

TPM	Host	Issuer
	$(X,\ Y) \in \mathbb{G}_2 \times \mathbb{G}_2$	$(x,\ y) \in \mathbb{Z}_n \times \mathbb{Z}_n$
	$v = H_5(n_J \parallel p_{tpm})$	
	$\sigma_{ch} = (n_J, w, v)$ $\xrightarrow{\mathcal{K}_1,\ \sigma_{ch}}$	$str = X \parallel Y \parallel \mathcal{K}_1 \parallel \mathcal{E}$
		extract Q_2 from Q_2PD
		$U' = [w]P_1 - [v]Q_2$
		$p' = H_2(P_1 \parallel Q_2 \parallel U' \parallel str)$
		$p'_{tpm} = H_{12}(p')$
		old
		$v' = p'_{tpm} \pmod n$
		new
		$v' = H_5(n_J \parallel p'_{tpm})$
		verify $v = v'$
		$r \leftarrow \mathbb{Z}_n$
		$A = [r]P_1;\ B = [y]A$
		$C = [x]A + [rxy]Q_2$
		$D = [ry]Q_2$
		$l \leftarrow \mathbb{Z}_n$
		$R_B = [l]P_1;\ R_D = [l]Q_2$
		$q = H_{10}(P_1 \parallel Q_2 \parallel R_B \parallel R_D)$

TPM		Host		Issuer
$(e, \mathcal{E}),\ f \in \mathbb{Z}_n$		$(X,\ Y) \in \mathbb{G}_2 \times \mathbb{G}_2$		$(x,\ y) \in \mathbb{Z}_n \times \mathbb{Z}_n$

$j = l + yr \cdot q \pmod{n}$

$s_2 \leftarrow \{0,1\}^t$

$cre = (A, B, C, D, q, j)$

$\mathcal{K}_2 \leftarrow \{0,1\}^{t_{aes}}$

$\widehat{\mathcal{C}} = \text{senc}(\mathcal{K}_2, cre)$

Issuer: generate CB_2 and $\widehat{s_2}$

Issuer → Host: $\text{CB}_2, \widehat{s_2}, \widehat{\mathcal{C}}$

Host: keep $\widehat{\mathcal{C}}$

Host → TPM: $\text{CB}_2, \widehat{s_2}$

ACTIVATE_CREDENTIAL

TPM: $\mathcal{K}_2 = \text{activate credential}(\text{CB}_2, \widehat{s_2})$

TPM → Host: $\mathcal{K}_2$

$cre = \text{senc}(\mathcal{K}_2, \widehat{\mathcal{C}})$

$(A, B, C, D, q, j) = cre$

$R'_B = [j]P_1 - [q]B$

$R'_D = [j]Q_2 - [q]D$

$q' = H_{10}(P_1 \parallel Q_2 \parallel R'_B \parallel R'_D)$

check :

$q = q'$

$\hat{h}(A, Y) = \hat{h}(B, P_2)$ and $\hat{h}(A + D, X) = \hat{h}(C, P_2)$

store (A, B, C, D)

Preleminary Results

- SIGN: 1538ms
- VERIFY: 2545ms

DEMO

Thank You!

Q/A

Twitter: @sudo_jorden
email: `j.whitefield@surrey.ac.uk`

JOIN Protocol

Join: TC	$\rightleftharpoons$	Host	$\rightleftharpoons$	Issuer
$sk_{ek_{tc}}, pk_{ek_{tc}}$		$pk_{ek_{tc}}, pk_{tc}$		$pk_{ek_{tc}}, sk_I$
sk_{tc}, pk_{tc}		pk_I		
			$\xrightarrow{pk_{ek_{tc}}, pk_{tc}}$	`fresh` n_I
	$\xleftarrow{C}$		$\xleftarrow{C}$	$C = \texttt{aenc}(n_I \Vert pk_{tc}, pk_{ek_{tc}})$
$n_I \Vert pk_{tc}$	$\xrightarrow{n_I \Vert pk_{tc}}$		$\xrightarrow{n_I \Vert pk_{tc}}$	$cre = \texttt{blindSign}(pk_{tc}, sk_I)$
				`fresh` key
				$e = \texttt{senc}(cre, key)$
	$\xleftarrow{d}$		$\xleftarrow{d,\ e}$	$d = \texttt{aenc}(key \Vert pk_{tc}, pk_{ek_{tc}})$
$key \Vert pk_{tc}$	$\xrightarrow{key}$	$\texttt{store}(cre)$		

CREATE Protocol

Create: Tc	$\rightleftharpoons$	Host
sk_{tc}		cre
		fresh r
fresh sk_{ps}/pk_{ps}	$\xleftarrow{\texttt{"create"} \parallel \widehat{cre}}$	$\widehat{cre} := \texttt{blind}(cre, r)$
fresh r'		
$ps_{sig} := \texttt{DAASign}(pk_{ps}, r', sk_{tc}) = (\sigma_1 \parallel \sigma_2 \parallel \widehat{cre})$		
$\sigma_1 := \texttt{sign}(pk_{ps}, sk_{tc})$		
$\sigma_2 := \texttt{blindSign}(\texttt{"certified"} \parallel pk_{ps}, r', sk_{tc})$		
$ps_{Cert_{tc}} := (pk_{ps} \parallel ps_{sig})$		
$\texttt{store}(sk_{ps})$	$\xrightarrow{ps_{Cert_{tc}}}$	$\texttt{store}(ps_{Cert_{tc}})$

SIGN/VERIFY Protocol

Sign / Verify: TC	$\rightleftharpoons$	HOST	$\rightleftharpoons$	VERIFIER
sk_{ps}		$psCert_{tc}$		pk_I
	$\xleftarrow{m_{plain}}$	$m_{plain} := \{\vert \text{"70 mph"} \parallel data \vert\}$		
$m_{sign} := \texttt{sign}(m_{plain}, sk_{ps})$	$\xrightarrow{m_{sign}}$	$msg := \{\vert\, m_{plain} \parallel m_{sign} \parallel psCert_{tc} \,\vert\}$	$\xrightarrow{msg}$	$\texttt{DAAVerify}(ps_{sig}, pk_I)$
				$\texttt{store}(pk_{ps})$

REVOKE Protocol

Revoke: Tc	$\rightleftharpoons$	Host	$\rightleftharpoons$	Ra
sk_{tc}, pk_{ra}		cre		$pk_I, pk_{ps}, psCert_{tc}, sk_{ra}$
				$msg := \{\| \texttt{"revoke"} \parallel pk_{ps} \parallel \texttt{reason} \|\}_{sk_{ra}}$
		$\texttt{fresh}\ r$	$\xleftarrow{msg}$	
$\texttt{verify}(msg, pk_{ra})$	$\xleftarrow{\widehat{cre}, msg}$	$\widehat{cre} = \texttt{blind}(cre, r)$		
$\texttt{fresh}\ r'$				
$\sigma_{rvk} := \texttt{DAASign}(pk_{ps}, r, sk_{tc}) = (\sigma_1^{ra} \parallel \sigma_2^{ra} \parallel \widehat{cre})$				
$\sigma_1^{ra} := \texttt{sign}(pk_{ps}, sk_{tc})$				
$\sigma_2^{ra} := \texttt{blindSign}(\texttt{"confirm"} \parallel pk_{ps}, r', sk_{tc})$	$\xrightarrow{\sigma_{rvk}}$	σ_{rvk}	$\xrightarrow{\sigma_{rvk}}$	$\texttt{eq}(\sigma_1, \sigma_1^{ra}, \texttt{true})$
				$\texttt{DAAVerify}(\sigma_{rvk}, pk_I)$