1) -Authentifizierung: Vertrauen in die Richtigkeit von Nachrichten, welche Entscheidungen bezüglich der Sicherheit betreffen.

-Datenintegrität: Daten nicht verändert wurden von einer unbefugten Partei

-Datenvertraulichkeit: Unautorisierte Inhalt von Nachrichten nicht lesen

-Erkennen von Fehlverhalten + Widerruf: Erkennen von Zertifikatsmissbrauch + Fehlfunktion, sowie die Fähigkeit diesen Fahrzeugen das Recht zu nehmen Nachrichten zu versenden, welche andere vertrauen würden.

2) Individuals, Loosely coordinated groups, Insiders, Adversary organisations, Foreign Governments, Government agencies

3) -Senden Falscher Sicherheitsnachrichten: Erzeugen unnötige Warnungen bei anderen Fahrzeugen.

-Unschuldige Fahrzeuge beschuldigen sich falsch zu Verhalten -> Erschwert das Finden von Fahrzeugen die sich tatsächlich falsch verhalten

-Initiieren von Fahrzeugen/Netzwerkentitäten: Andere Fahrzeugen vorgaukeln es wären mehr Autos in der Nähe als es tatsächlich sind -> z.B. Direkt vor einem am Bremsen

- Denial of Service (DoS): Deaktivieren/stören der Kommunikationfähigkeit anderer Fahrzeuge

4) Kryptographische algorithmen/protokolle, Sicherheitsunterstützende Mechanismen

5) Daten in Geheimtext umwandeln um seine Bedeutung zu verheimlichen

6) Sym.: Ver-/Entschlüsseln mit dem selben Schlüssel

Asym.: Versch. mit Pub. Key, Entsch. mit Priv. Key

7) Hash des Klartext berechnen -> Versch. mit Pub. Key -> Mit Nachricht versenden -> Hash entsch. -> Vergleichen mit Hash empf. Nachricht

8) Sichert das Zertifikat eines Fahrzeugs ab, da man dieser Zertifizierungsstelle vertrauen kann -> Pub. Key bereits vorinstalliert, Signierung mit Priv. Key

9) Enthält min. Name + Pub. Key des Besitzers

+ Protokol Version, Seriennummer Zertifikat, Gültigkeitszeitraum, Zertifikat Zertifizierungsstelle

10) Verteilen von Zertifikaten an alle Teilnehmende

11) 1) Root Zertifizierungsstelle (RCA) -> Zertifizieren sich gegenseitig

2) Langzeit (LTCA) + Pseudonym (PCA) -> Vertrauenspfad zu den RCA

3) ITS Centre/Roadside/Vehicle Station -> erhalten Zert. von LTCA/PCA

12) RCA: Definieren einheitliche Richtlinien auf alle LTCA's + PCA's

LTCA: Ausgabe LTC's an ITS Stationen

PCA: Authorisiert von RCA, Ausgabe PC's an ITS Stationen

13) -Gleichmäßiges Vertrauen + Kosteneffizient der RCA

- Flexibilität bei Prozessintegration -> Neue Hersteller führen eigene LTCA unter Europäischen RCA + Organisation liefert PCA für alle Hersteller

- Flache Strukture -> Nur ein Zert. pro Nachricht

14) Privatsphäre der Position/Interessen/Sozialer Status/Privatleben

15) Identitäten sind an Fahrzeuge gebunden

16) Durch Benutzung mehrerer Identitäten anstatt einer -> Verfolgen schwierig, immer andere Identität

17) 1. PCA weisen Basisidentität Automobil Industrie zu

2. Diese weisen eine " pro neuem Fahrzeug zu

3. Fahrzeuge erstellen selbst pool von p versch. Pseudonymen in Form von Zertifikatsanfragen

4. " Fragen bei PCA signierung jedes Pseudonyms an über Internet

5. PCA überprüft Anfrage -> falls korrekt, sende signiertes Pseudonym zurück

18) Komplett zufällig, Periodisch, Geographisch, Fahrzeugwerte/Kommunikationsqualität, Silent Periods

19) Overhead -> Jedes CAM müsste 150-160 Byte zusätzlich groß sein für Signatur etc. -> enorm großer Datenfluss nur für Sicherheit

-> Jedes CAM muss ver-/entsch. werden enorm häufig