

SmartMove

The Common Platform For Vehicle Communication

Danny De Cock

ESAT/COSIC

17th February 1999

Outline

- SmartMove – What is it?
- How does it work?
- Example
- What are SmartMove's goals and constraints?
- Why does SmartMove need security?
- Candidates to guarantee data-integrity
 - RSA
 - DSA
 - ECC
- Certificate requirements
 - What about X.509, IETF, ...?
 - What about IEEE P1363, ISO 9796-2?
 - What about EMV?
- About key establishment protocols
 - Key transport with PK-encryption, without signatures
 - Key transport with PK-encryption and signatures
 - Key agreement with PK-techniques
- Bibliography

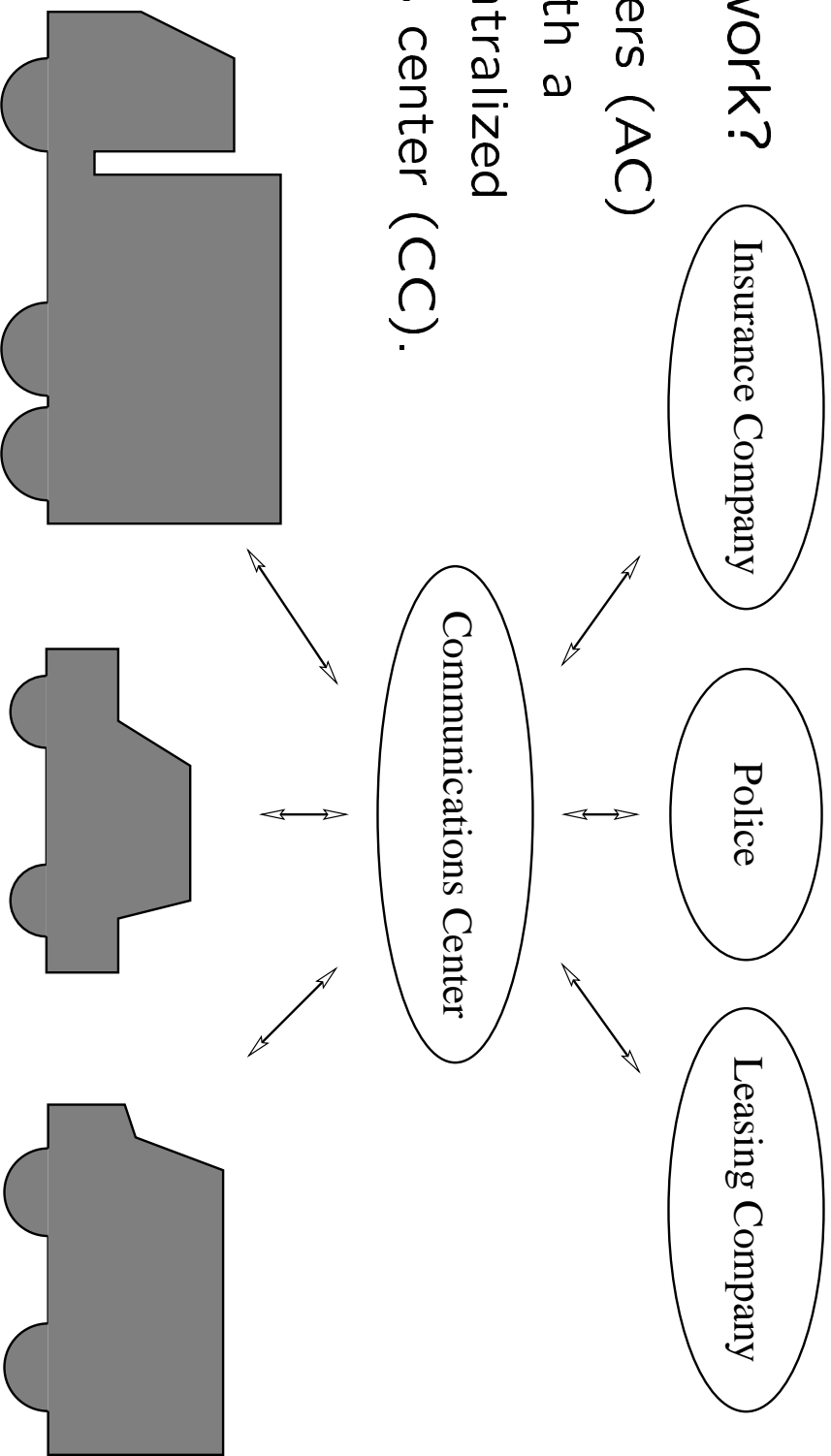
SmartMove – What is it?

A system built into a car which provides

- navigation support
- fleet management
- traffic information
- emergency assistance
- on-board diagnostics
- theft control
- ...

How does it work?

Application centers (AC) communicate with a centralized Communications center (CC).



What are SmartMove's goals and constraints?

The communications system offers a service which is:

- reliable: why should one design a non-reliable system?
- flexible device allocation:
 - bidirectional: GSM, DSRC
 - unidirectional: ERMES
- secure: protection against tampering of data and eavesdroppers

Constraints:

- bandwidth of the communication channels used

Why does SmartMove need security?

- Examples which need data integrity:
 - sending speed, position, on-board diagnostics, fuel consumption, alarm status,... to an AC
 - receiving instructions, de-activation requests, new applications,... from an AC or the CC
- Examples which need confidentiality:
 - vehicle identification, speed, position, on-board diagnostics, traffic information,...
 - de-activation requests, toll collection,...

Candidates to guarantee data-integrity

- cryptographic hash function (RIPEMD-160, SHA-1,...)
- MAC-based system (MDX-MAC, HMAC,..) provides
 - both data integrity and data origin authentication,
 - no non-repudiation, but
 - requires tamper resistant storage and processing devices
- digital signature (RSA, DSA, ECC,...) provides
 - data integrity, data origin authentication, non-repudiation
 - high flexibility, but
 - requires certificate management
 - requires tamper resistant storage and processing devices

RSA

- Advantages:
 - fast signature verification
 - ≈ 0.65 ms (1024-bit modulus, 3-bit exponent) on a PPro200
 - patent expires in September, 2000
 - well known, de facto standard
 - ISO 9796-2: ≈ 1024 bits+24 bytes
- Disadvantages:
 - slow signature generation ≈ 43.3 ms
 - long keys to provide long-term security (≥ 1024 bits)

DSA

- Advantages:
 - few patent problems
 - well known
 - short signatures (320 bits)
 - fast signature generation ≈ 7 ms (1024-bit modulus)
- Disadvantages:
 - medium speed signature verification (≈ 28.3 ms)
 - requires a source of randomness
 - long keys to provide long-term security (≥ 1024 bits) parameters ≥ 2048 bits

ECC

- Advantages:
 - short keys provide long-term security (≈ 200 bits)
 - fast signature generation
 - ≈ 11.3 ms over $GF(2^n)$ (191-bit modulus)
 - ≈ 6.3 ms over $GF(p)$
 - medium signature size (≈ 400 bits)
- Disadvantages:
 - slow signature verification
 - ≈ 60 ms in $GF(2^n)$
 - ≈ 26 ms in $GF(p)$
 - requires a source of randomness
 - patent situation unclear
 - ‘recently’ introduced in cryptography
(Neal Kobitz and Victor Miller, 1985)

Certificate requirements

Minimum information:

- identification number
- public verification key
- owner's characteristics
- information about the certificate issuer
- validity period
- certificate version, signature

Mobile application

- ⇒ minimize communications overhead
- ⇒ preferably short certificates

What about X.509, IETF, ...?

- Description:
 - generic certificate description language
 - contains much redundancy
- Advantages:
 - well known, de facto standard
 - widely used on the Internet
- Disadvantages:
 - too large: \approx 1000 bytes for a typical public-key certificate
 - too complex: ASN.1

What about IEEE P1363, ISO 9796-2?

- Description:
 - encodes the data which must be signed
- Advantages:
 - hides structures of the actual data
- Disadvantages:
 - IEEE P1363 standard is still subject to change
 - P1363 requires a source of randomness
 - ISO 9796-2 is only suited for RSA-based signatures

What about EMV?

- Description:
 - straightforward certificate format
 - designed for smartcard applications
- Advantages:
 - low overhead
 - simple
- Disadvantages:
 - not widely known
 - not usable with off the shelf applications, browsers,...

About key establishment protocols

- definition: a multi-party algorithm, defined by a sequence of steps precisely specifying the actions required of two or more parties in order to achieve a specified objective
- objectives:
 - entity authentication, key authentication
 - e.g., key transport
 - key establishment
 - e.g., Diffie-Hellman
 - authenticated key establishment
 - e.g., Station-to-Station, Menezes-Qu-Vanstone
- desirable features:
 - perfect forward secrecy: compromise of a long term private key pre-serves secrecy of previous session keys
 - joint key control

Key transport with PK-encryption, without signatures

- One-pass key transport:
 - $A \rightarrow B : P_B(k)$
 - implicit key authentication
- Needham-Schroeder (3-passes):
 - $A \rightarrow B : P_B(k_1 \| A)$
 - $A \leftarrow B : P_A(k_1 \| k_2)$
 - $A \rightarrow B : P_B(k_2)$
 - $k = f(k_1 \| k_2)$
 - mutual key and entity authentication

Key transport with PK-encryption and signatures

- One-pass key transport:
 - $A \rightarrow B : P_B(k \| S_A(B \| k))$
 - implicit key authentication, explicit source authentication
- Two-pass key transport: Beller-Yacobi
 - $A \rightarrow B : r_A \| cert_A$
 - $A \leftarrow B : P_A(k) \| E_k(cert_B \| w)$
(v, k) is B 's ElGamal signature on $(r_A \| A)$
 - A obtains entity authentication of B
 - B has key authentication with respect to A

Key transport with PK-encryption and signatures (ctd)

- Three-pass key transport: Beller-Yacobi (extension)
 - $A \rightarrow B : r_A \parallel cert_A$
 - $A \leftarrow B : P_A(k) \parallel E_k(cert_B \parallel w)$
 - $A \rightarrow B : E_k(r_A)$
 - explicit key authentication for B of A (implying entity authentication)
- Four-pass key transport: Beller-Yacobi
 - protocol description intentionally skipped
 - mutual entity authentication, explicit key authentication
 - B only executes inexpensive operations

Key agreement with PK-techniques

- Diffie-Hellman (2 passes)
 - $A \rightarrow B : \alpha^x \bmod p$
 - $A \leftarrow B : \alpha^y \bmod p$
 - $k = \alpha^{xy} \bmod p$
 - no key authentication, no entity authentication
- ElGamal (1 pass)
 - $A \rightarrow B : \alpha^x \bmod p$
 - $k = \alpha^{xb} \bmod p$
 - Assumption: A has already B 's public key (p, α, α^b)
 - unilateral key authentication
 - no entity authentication, no key confirmation
 - no key freshness assurance

Key agreement with PK-techniques (ctd)

- MTTI/A0 (Matsumoto, Takashima, Imai, 2 passes)
 - Diffie-Hellman, using long-term secrets also
 - A computes $k = (\alpha^y)^a (z_B)^x \bmod p$, $z_A = \alpha^a \bmod p$
 - B computes $k = (\alpha^x)^b (z_A)^y \bmod p$, $z_B = \alpha^b \bmod p$
 - $k = \alpha^{bx+ay} \bmod p$
 - mutual key authentication
 - no key confirmation, no entity authentication
 - secure against passive attacks
 - vulnerable to active attacks
- Station-to-Station (3 passes)
 - $A \rightarrow B : \alpha^x \bmod p$
 - $A \leftarrow B : \alpha^y \bmod p \parallel E_k(S_B(\alpha^y \parallel \alpha^x))$
 - $A \rightarrow B : E_k(S_A(\alpha^x \parallel \alpha^y))$
 - $k = \alpha^{xy} \bmod p$
- mutual entity authentication, explicit key authentication

Key agreement with PK-techniques (ctd²)

- Menezes-Qu-Vanstone (MQV, 2 passes)
 - protocol description intentionally skipped
 - based on Diffie-Hellman
 - mutual entity authentication
 - mutual implicit key authentication
 - no key confirmation
- MQV, 3 passes
 - extension of MQV with 2 passes
 - key confirmation

Bibliography

- M. Bellare, Ph. Rogaway, "Optimal Asymmetric Encryption," *Advances in Cryptology—Crypto '94*, LNCS 950, pp. 92-111, 1994.
- D. Bleichenbacher, "Generating ElGamal signatures without knowing the secret key," *Advances in Cryptology, Proceedings Eurocrypt'96*, LNCS 1070, Ueli Maurer, Ed. Springer Verlag, 10-18, 1996.
- T. Denny, B. Dodson, A.K. Lenstra, M.S. Manasse, "On the factorization of RSA-120," *Advances in Cryptology—Crypto '93 (LNCS 773)*, 166-174, 1994.
- J. Daemen, L.R. Knudsen and V. Rijmen, "The block cipher Square," *Fast Software Encryption, LNCS 1267*, E. Biham, Ed., Springer-Verlag, 1997, pp. 149–165.
- J. Daemen, L. R. Knudsen and V. Rijmen, "The Square Encryption algorithm," *Dr. Dobb's Journal*.
- FIPS 180-1, "Secure Hash Standard," Federal Information Processing Standard (FIPS), Publication 180-1, National Institute of Standards and Technology, US Department of Commerce, Washington D.C., April 1995.
- IEEE P1363 Working Draft, October 5th, 1998.
- N. Kobitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, 48 (1987), 203-209.
- T. Leighton, S. Micali, "Secret-Key Agreement without Public-Key Cryptography (Extended Abstract)," *Advances in Cryptology—Crypto '93*, LNCS 773, 1993, pp. 456-479.
- B. Preneel, P. Van Oorschot, "MD α -MAC and building fast MACs from hash functions," *Advances in Cryptology – Crypto'95*, LNCS 963, 1995, pp. 1-14.
- V. Miller, "Uses of elliptic curves in cryptography," *Advances in Cryptology – Crypto '85*, Lecture Notes In Computer Science, 218 (1986), Springer-Verlag, 417-426.
- A. Bosselaers, B. Preneel, editors, "Integrity Primitives for Secure Information Systems: Final Report of RACE Integrity Primitives Evaluation RIPE-RACE 1040," LNCS 1007, Springer-Verlag, New York, 1995.
- H. Dobbertin, A. Bosselaers, B. Preneel, "RIPEMD-160: a strengthened version of RIPEMD," D. Gollmann, editor, *Fast Software Encryption, Third International Workshop*, LNCS 1039, pp. 71-82, Springer-Verlag, 1996.
- R.L. Rivest, A. Shamir, L.M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, 21 (1978), 120-126.
- Yuliang Zheng, "How to Break and Repair Leighton and Micali's Key Agreement Protocol," *Advances in Cryptology—Eurocrypt '94*, LNCS 950, 1994, pp. 299-305.