HIMMO

Oscar Garcia-Morchon, Ronald Rietman, Ludo Tolhuizen

July 2016

innovation + you

PHILIPS

Aims of the presentation

- To share work done at Philips Research
- To discuss rationale of HIMMO
- To get feedback on our work

PHILIPS

Contents

- Key Pre-Distribution Schemes
- HIMMO
- The HIMMO Contest
- Performance

PHILIPS

Key Pre-Distribution Scheme

A key pre-distribution scheme involves a trusted third party TTP and nodes $N_1, \ldots, N_l$ and consists of the following three components.

- **Setup.** An algorithm run by TTP for generating secret root keying material R and public system parameter P, given a security parameter.
- **Extract.** An algorithm run by TTP for generating secret keying material s_x for a given node N_x, given root keying material R and system parameter P.
- **Key establishment.** A protocol run by node N_x and N_y for generating shared key $k_{x,y}$, given secret keying material s_x and s_y, and system parameter P.

PHILIPS

Rationale

Features of KPS

- ✓Efficient
- ✓Any node can directly obtain a pairwise key with any other any node
- ✓Based on identities so that it is possible to verify them
- ✓Multiple TTP support so that a single TTP does not have access to all keys
- X KPS collusion resistance

Our goal with HIMMO was to achieve collusion resistance while keeping the rest of nice features

HIMMO

- **Setup.**
  - Determine positive integers b, m, u, t for a given security parameter
  - Let N be an odd integer of bit length $3b$
  - Let $q_i = N - \beta_i 2^b$ for β_i being a secret b bit positive integer, for $0 \leq i \leq\ m-1$
  - Let $\boldsymbol{R_i}$ be a random symmetric $t\ x\ t$ matrix over Z_{q_i}, for $0 \leq i \leq\ m-1$
- **Extract.**
  - Associate node N_x with a public random vector identifier $\boldsymbol{x} \in [1,2^b]^t$
  - TTP provides node N_x with secret key generating vector $\boldsymbol{s_x} = \left\langle \sum_{i=0}^{m-1} \langle \boldsymbol{x R_i} \rangle_{q_i} \right\rangle_N$
- **Key establishment.**
  - N_x computes $s_{x,y} = \left\langle \langle \boldsymbol{s_x y}^T \rangle_N \right\rangle_{2^b}$ and determines $k_{x,y} = \left\lfloor \frac{s_{x,y}}{2^u} \right\rfloor$ and $h = \left\langle s_{x,y} \right\rangle_{2^u}$
  - N_x sends h to N_y
  - N_y computes $k_{x,y}$ from $k_{y,x}$ and h as $\left\lfloor \frac{\left\langle K_{y,x} + \lambda N \right\rangle_{2^b}}{2^u} \right\rfloor$ where $\lambda = \left\{ N^{-1} \left(h - k_{y,x} \right) \right\}_{2^u}$

- O. Garcia-Morchon, L. Tolhuizen, D. Gomez, and J. Gutierrez. Towards full collusion resistant ID-based establishment of pairwise keys. In Extended abstracts of the third Workshop on Mathematical Cryptology (WMC 2012) and the third international conference on Symbolic Computation and Cryptography (SCC 2012). Pages 30-36, 2012.
- O. Garcia-Morchon, D. Gomez-Perez, J. Gutierrez , R. Rietman, B. Schoenmakers, and L. Tolhuizen,. HIMMO - A Lightweight, Fully Collusion Resistant Key-Pre-distribution Scheme. Cryptology ePrint Archive, Report 2014/698.
- O. Garcia-Morchon, R. Rietman, L. Tolhuizen, J.L. Torre-Arce, M.S. Lee, D. Gomez-Perez, J. Gutierrez, B. Schoenmakers, "Attacks and parameter choices in HIMMO", ", IACR ePrint Archive, Report 2016-152

$\langle x \rangle_m$ is the integer in $[0, x)$ such that $x \equiv \langle x \rangle_m \ (mod\ m)$

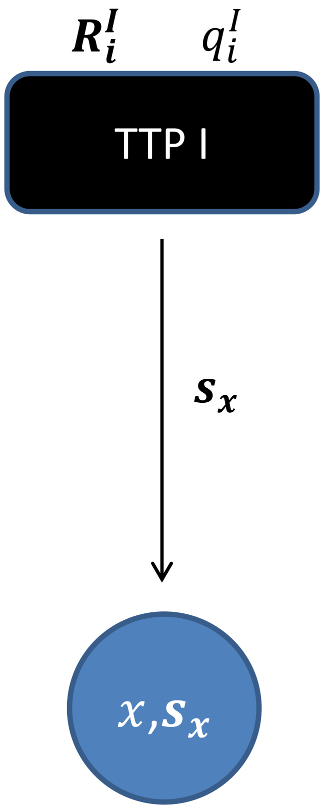
HIMMO

- **Setup.**
  - Determine positive integers b, m, u, t for a given security parameter
  - Let N be an odd integer of bit length $3b$
  - Let $\boxed{q_i} = N - \beta_i 2^b$ for β_i being a secret b bit positive integer, for $0 \leq i \leq m-1$
  - Let $\boxed{\boldsymbol{R_i}}$ be a random symmetric $t\ x\ t$ matrix over Z_{q_i}, for $0 \leq i \leq m-1$
- **Extract.**
  - Associate node N_x with a public random vector identifier $\boldsymbol{x} \in [1,2^b]^t$
  - TTP provides node N_x with secret key generating vector $\boldsymbol{s_x} = \left\langle \sum_{i=0}^{m-1} \langle \boldsymbol{x}\boldsymbol{R_i} \rangle_{q_i} \right\rangle_N$
- **Key establishment.**
  - N_x computes $s_{x,y} = \left\langle \langle \boldsymbol{s_x} \boldsymbol{y}^T \rangle_N \right\rangle_{2^b}$ and determines $k_{x,y} = \left\lfloor \frac{s_{x,y}}{2^u} \right\rfloor$ and $h = \left\langle s_{x,y} \right\rangle_{2^u}$
  - N_x sends h to N_y
  - N_y computes $\boxed{k_{x,y}}$ from $k_{y,x}$ and h as $\left\lfloor \frac{\langle K_{y,x} + \lambda N \rangle_{2^b}}{2^u} \right\rfloor$ where $\lambda = \left\{ N^{-1} \left(h - k_{y,x} \right) \right\}_{2^u}$

- O. Garcia-Morchon, L. Tolhuizen, D. Gomez, and J. Gutierrez. Towards full collusion resistant ID-based establishment of pairwise keys. In Extended abstracts of the third Workshop on Mathematical Cryptology (WMC 2012) and the third international conference on Symbolic Computation and Cryptography (SCC 2012). Pages 30-36, 2012.
- O. Garcia-Morchon, D. Gomez-Perez, J. Gutierrez , R. Rietman, B. Schoenmakers, and L. Tolhuizen,. HIMMO - A Lightweight, Fully Collusion Resistant Key-Pre-distribution Scheme. Cryptology ePrint Archive, Report 2014/698.
- O. Garcia-Morchon, R. Rietman, L. Tolhuizen, J.L. Torre-Arce, M.S. Lee, D. Gomez-Perez, J. Gutierrez, B. Schoenmakers, "Attacks and parameter choices in HIMMO", ", IACR ePrint Archive, Report 2016-152

HIMMO in practice

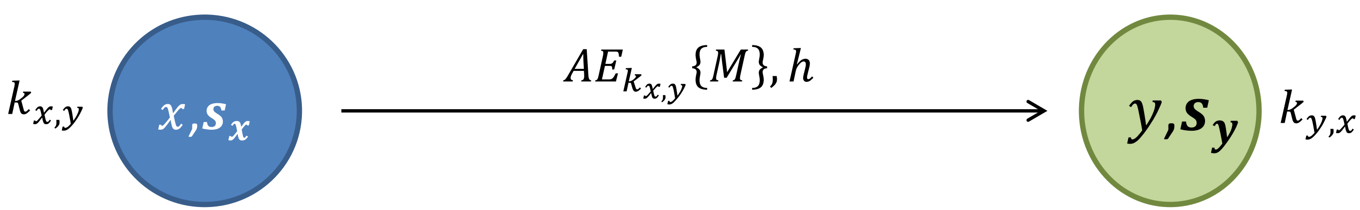
Extraction



PHILIPS

HIMMO in practice

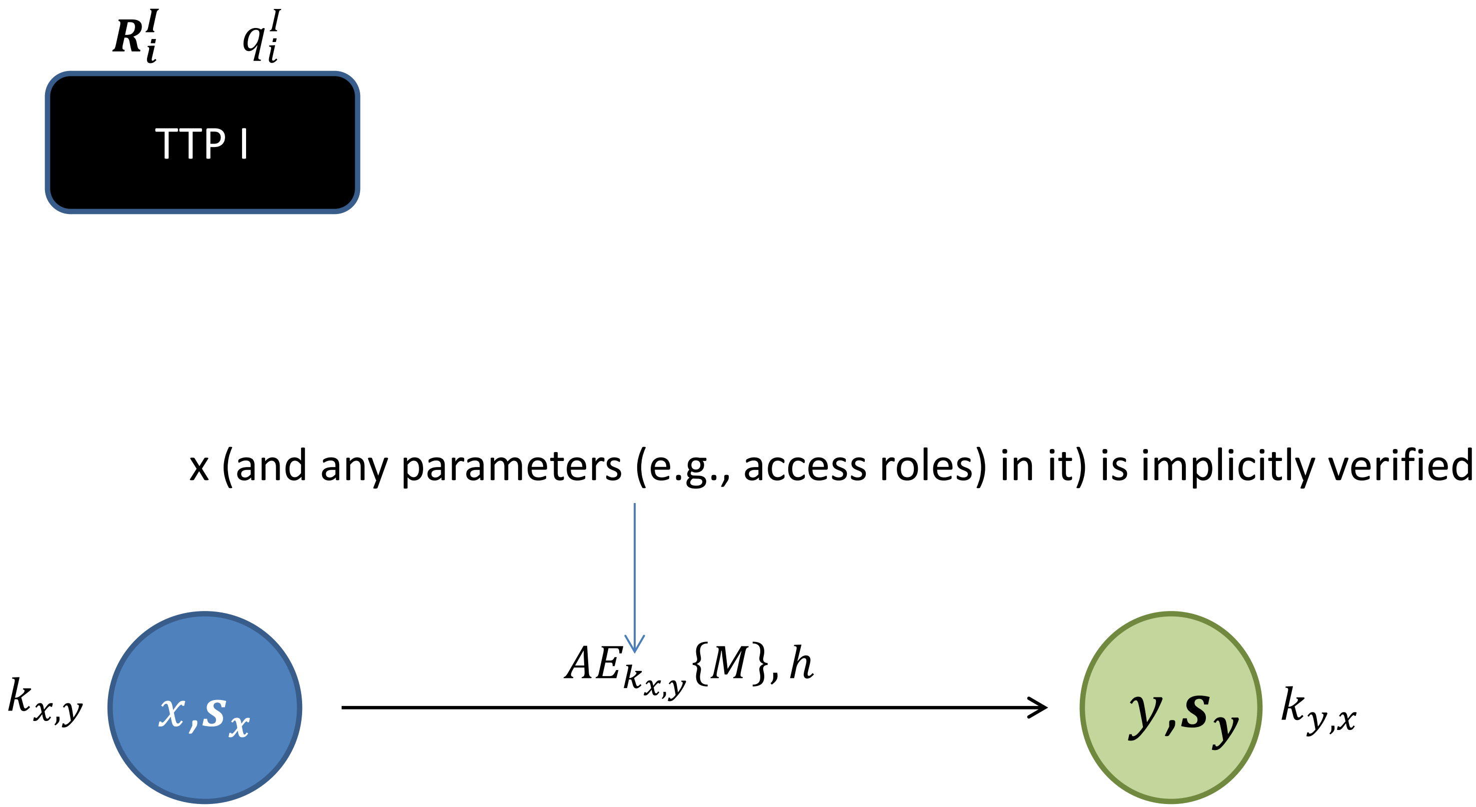
One-way key exchange and entity authentication



PHILIPS

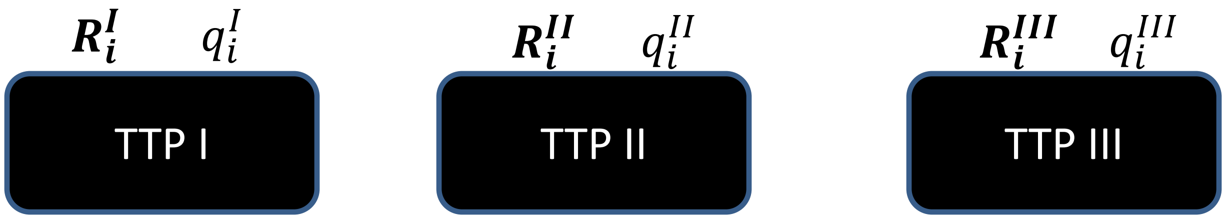
HIMMO in practice

Implicit certification and verification of parameters



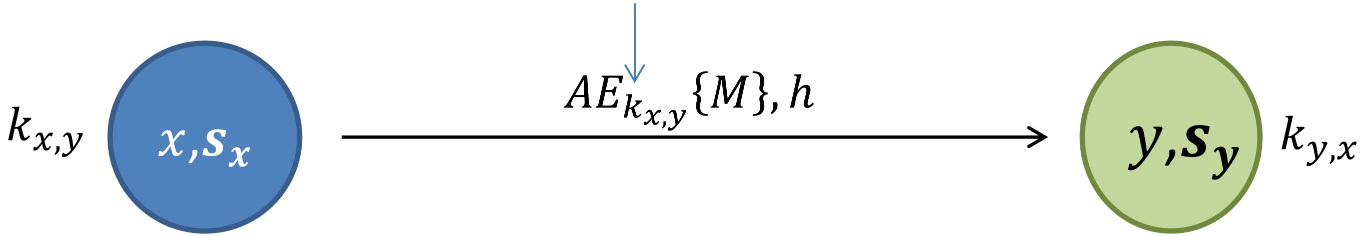
HIMMO in practice

Multiple TTP support



x (and any parameters (e.g., access roles) in it) is implicitly verified

Single TTP does not have access to communication

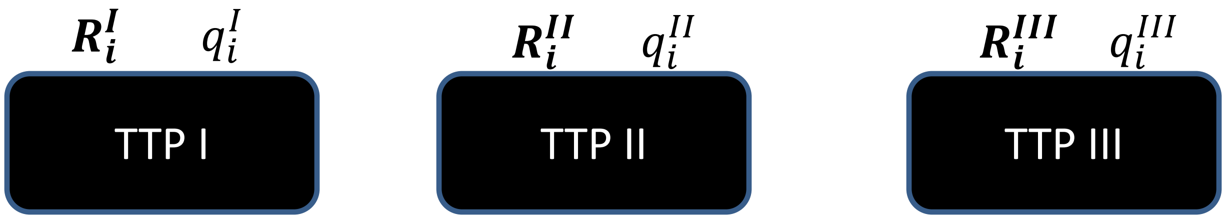


O. Garcia-Morchon, R. Rietman, S. Sharma, L. Tolhuizen, J.L., Torre-Arce. DTLS-HIMMO Efficiently Securing a Post-Quantum World with a Fully-Collusion Resistant KPS. In ESORICS 2015; also presented at NIST workshop on Cybersecurity in a Post-Quantum World, 2015.

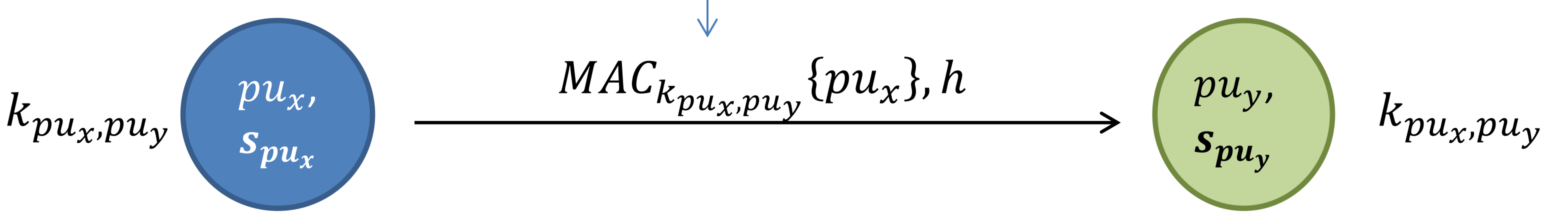
PHILIPS

HIMMO in practice

HIMMO for certification of public-keys



Single TTP cannot fake the MAC that verifies x’s public key (pu_x)



O. Garcia-Morchon, R. Rietman, L. Tolhuizen, J.L. Torre-Arce, S. Bhattacharya and M. Bodlaender "Efficient quantum-resistant trust Infrastructure based on HIMMO", IACR ePrint Archive, Report 2016-410

PHILIPS

Attacks paths and security analysis

- Eve has any set of c compromised keying materials $\boldsymbol{s}_{\boldsymbol{x}_1}, \dots, \boldsymbol{s}_{\boldsymbol{x}_c}$. Eve's goal is to find the key shared between Alice and Bob, $k_{a,b}$.
- Attack paths:
  - Try to recover $k_{a,b}$ by attacking the TTP: recovers $\boldsymbol{R}_{\boldsymbol{i}}$, q_i, $\boldsymbol{s}_{\boldsymbol{x}}$, and any $k_{x,y}$.
  - Try to recover $k_{a,b}$ by attacking Alice's $\boldsymbol{s}_{\boldsymbol{a}}$ (or Bob): recovers $\boldsymbol{s}_{\boldsymbol{a}}$, and any $k_{a,y}$.
  - Try to recover $k_{a,b}$ only.
- Security analysis for the above attack paths is described here

  O. Garcia-Morchon, R. Rietman, L. Tolhuizen, J.L. Torre-Arce, M.S. Lee, D. Gomez-Perez, J. Gutierrez, B. Schoenmakers, "Attacks and parameter choices in HIMMO", ", IACR ePrint Archive, Report 2016-152

HIMMO

Security analysis relies on the HI and MMO problems

HI [1]: given arbitrarily many keys and corresponding reconciliation data, recovering the keying material of a node or the key of another pair is computationally infeasible

$$s_{x,y} = \left\langle \langle \boldsymbol{s}_{\boldsymbol{x}} \boldsymbol{y}^T \rangle_N \right\rangle_{2^b}$$

MMO [2]: given the keying materials of arbitrarily many nodes, recovering the root keying material or estimating the keying material of another node is computationally infeasible

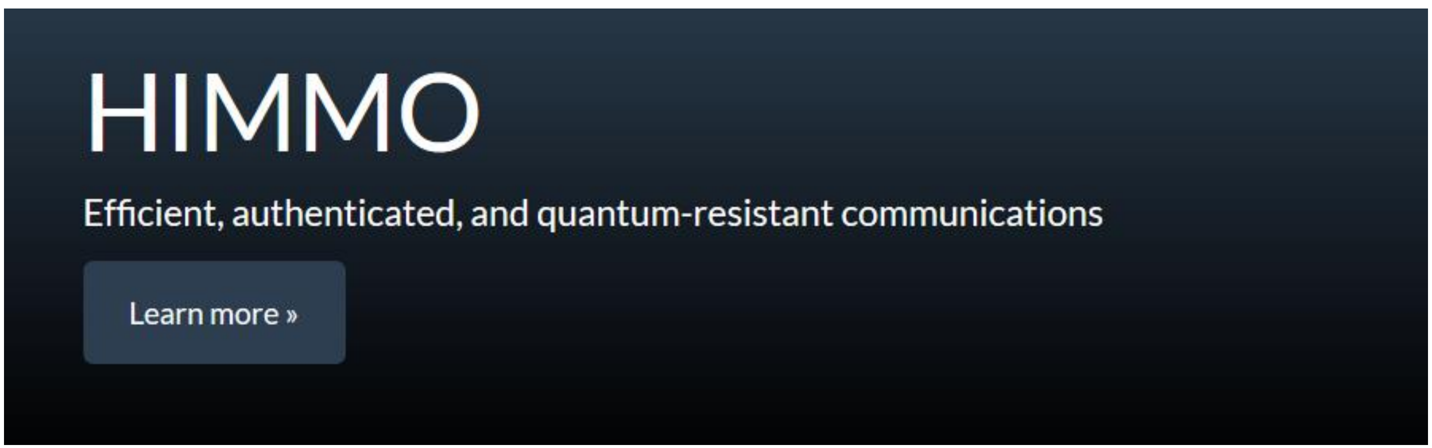
$$\boldsymbol{s}_{\boldsymbol{x}} = \left\langle \sum_{i=0}^{m-1} \langle \boldsymbol{x} \boldsymbol{R}_{\boldsymbol{i}} \rangle_{q_i} \right\rangle_N$$

[1] O. Garcia Morchon, Ronald Rietman, Igor E. Shparlinski, and Ludo Tolhuizen. Interpolation and approximation of polynomials in finite fields over a short interval from noisy values. Experimental mathematics, 23:241–260, 2014.

[2] O. Garcia-Morchon, D. Gomez-Perez, J. Gutierrez, R. Rietman, and L. Tolhuizen. The MMO problem. In Proc. ISSAC'14, pages 186–193. ACM, 2014.

HIMMO Contest

www.himmo-scheme.com



PHILIPS

Public verification and the HIMMO Contest

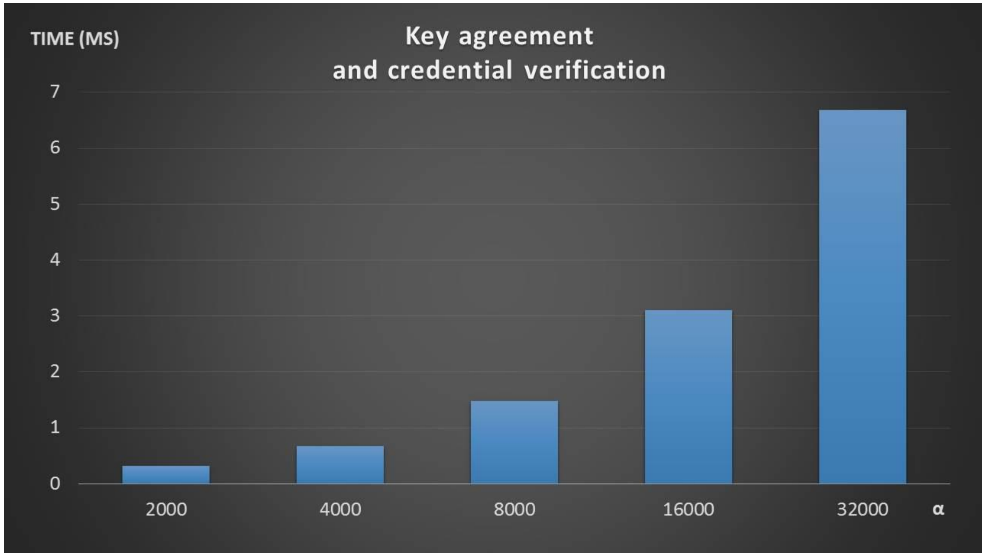
- Since 2012 we have tried to get as much public feedback as feasible talking and receiving feedback during crypto-colloquiums: Leuven, TU/e, Bochum, Darmstadt, DTU, MIT, Saarland, Paris, NIST, and many others.
- We announced the contest during NIST Workshop on PQ crypto (early 2015)
  – ~ 34 times downloaded
- So far HIMMO has received attention (review) not only from academia, but also several national security agencies (at least 2) and several industrial corporations have reviewed/worked on it or are reviewing/working on it now.
- Software implementation for research purposes available

PHILIPS

About the HIMMO Contest

- No time limit, you can take as much time as you need
- Five challenges for $b = 32$
- 1000 Euros per solved challenge

Challenge	t
HIMMO1	2000
HIMMO2	4000
HIMMO3	8000
HIMMO4	16000
HIMMO5	32000



PHILIPS

Performance

	Classical	Quantum
Size of the generated key (bits)	**80**	**256**
Target security level (bits)	**80**	**128**
m	10	21
b (bits)	32	32
t	2750	4000
Number of HIMMO instances	5	19
Identity size (Bytes)	10	32
“Signature size” (Bytes)	10	32
One-way key exchange (Bytes)	**20**	**75**
One-way key exchange & entity authentication (Bytes)	**30**	**107**
PC time (ms)	0.29	0.68
NXP 120 MHz time (ms)	18.45	41.37
Required Root Hermite factor (best attack)	1.008	1.0056
Pre-processing running time for LLL (years)	75	639.65

Thanks!!

Q&A

PHILIPS

Two Applications

- Integration of HIMMO into (D)TLS-PSK
  - Low communication overhead
  - Mutual authentication
  - Capabilities of digital certificates
- HIMMO as trust infrastructure for verifying public-keys
  - Public-keys are HIMMO identities
  - Implicit verification of public-keys relying on multiple TTPs
  - Does not require the exchange of certificates

[5] O. Garcia-Morchon, R. Rietman, S. Sharma, L. Tolhuizen, J.L., Torre-Arce. DTLS-HIMMO Efficiently Securing a Post-Quantum World with a Fully-Collusion Resistant KPS. In ESORICS 2015; also presented at NIST workshop on Cybersecurity in a Post-Quantum World, 2015.

[9] O. Garcia-Morchon, R. Rietman, L. Tolhuizen, J.L. Torre-Arce, S. Bhattacharya and M. Bodlaender "Efficient quantum-resistant trust Infrastructure based on HIMMO", IACR ePrint Archive, Report 2016-410