A Lightweight Inter-domain Direct Anonymous Attestation Scheme for Machine-to-Machine Networks

Liquan Chen, Aiqun Hu, Jie Huang
School of Information Science and Engineering
Southeast University, Nanjing, P. R. China
E-mail: Lqchen@seu.edu.cn

Johanna Virkki
Dept. of Electronics
Tampere University of Technology, Tampere, Finland
E-mail: Johanna.virkki@tut.edu.fi

Abstract— **As an important application mode of Internet of Things, Machine-to-Machine (M2M) networks have gained more and more concerns. However, the security problems such as privacy protection and platform authentication in M2M networks are not fulfilled the requirements yet. Since the M2M devices are always assigned to desolate and uninhabited circumstances, it is vulnerable to be stolen or maliciously attacked by those adversary or hacker. Meanwhile, the limiting computational and storage capabilities of M2M device also restrain the application of complicated security scheme. The inter-domain platform authentication of M2M device belonged to different issuer is not fully resolved in those early literatures. In this paper, we propose a Lightweight Inter-domain Direct Anonymous Attestation (L-IDAA) scheme to solve the security problems in inter-domain M2M networks according to the features of them and the characters of the M2M devices. We build a M2M Certificate Authority system above the issuer domains, and use this CA system to assure the authenticity of Issuers and Verifiers in different DAA domains. The proposed scheme can remedy the security fault of those legacy inter-domain schemes and gain higher computational efficiency. The computational cost for TPM is reduced to $1G_1^2$ and that for Host is reduced to $16G_1+1G_1^2$. Finally, we use the ideal/real-system model to prove the security of L-IDAA scheme. The results show that the proposed L-IDAA scheme is feasible and is suitable for inter-domain anonymous attestation in M2M networks.**

Index Terms—Direct Anonymous Attestation, Machine-to-Machine, Inter-domain Attestation, Lightweight, Trusted Platform Module

I. INTRODUCTION

In M2M networks, there are different independent trusted domains for Direct Anonymous Attestation (DAA) [1]. Every trusted domain has its own trusted DAA certificate issuer. The DAA certificate based on one Trusted Platform Module (TPM) is trusted only in its own domain, but not trusted in the other network domains. When the trusted platforms and the verifiers are in different domains, verifier in one trusted domain does not trust the certificates published in the other trusted domain. So, the traditional single-domain DAA protocols can't function normally in inter-domain circumstance [1, 2]. In M2M networks, there are large numbers of M2M end devices and they are dispersedly distributed in various environments. However, all these M2M end devices, which lie in different domains, generally need the inter-domain platform legality verification. It is necessary to propose a suitable DAA algorithm for M2M inter-domain anonymous attestation to meet the security demand of M2M inter-domain attestation [3-8].

Here, there has been no published literature related to inter-domain DAA scheme based on Elliptic Curve Cryptosystem (ECC). And that related to inter-domain attestation for M2M has not been found yet. Based on full consideration of the security needs and efficiency requirements of M2M networks, a Lightweight Inter-domain Direct Anonymous Attestation (L-IDAA) is proposed in this paper. With high security and efficiency, the proposed L-IDAA scheme, which is based on ECC-DAA mechanism [9-12], is suitable for M2M devices which have limited computational capability and transmission bandwidth. Moreover, it is an effective scheme to fulfill trusted platform attestation among different domains and bring wide application for M2M networks.

II. ANALYSIS AND COMPARISON OF THOSE EXISTING INTER-DOMAIN DAA SCHEMES

The BCC-DAA scheme presented in TPM specification v1.2 is only fit for those inner networks and single trusted domain. It can't provide identity authentication for the trusted platforms among different DAA trusted domains [1]. Then, an inter-domain DAA model is proposed in ref. [8]. It adds two entities in each authentication domain: passport issuer and visa issuer. HostA should first apply a passport certificate from its own certificate issuer and then apply a visa certificate from the visa issuer of Domain B. Only with possession of the two certificates, VerifierB in domain B can trust the identity of HostA. However, in ref. [8], the specific solution on how the signing issuer of one domain trusts the passport issuer of another domain is not provided yet. In ref. [14], issuers in two domains build agency relationship by exchanging their public keys in order to deal with the distrust between two domains. However, it is unreasonable for one trusted platform to apply certificates from different issuers with the same secret value. If TPM owns several certificates issued by different I ssuer at the same time, the secret values of the different certificates should not be the same. So, it is unreasonable to use the same secret value of domain A's certificate to issue Domain B's certificate. Consequently, the scheme of [14] can't solve the distrust problem among different trusted domains. Then, ref. [15] proposes a new scheme to solve the distrust problem among different trusted domains. It is based on the inter-domain authentication model of ref. [1], and adds a third Trusted Auditor (TA) above DAA trusted domains. TAs in different domains mutually authenticates with each other and shares the same secret key K. Then, TA-A in domain A firstly

© 2013. The authors - Published by Atlantis Press

verifies the DAA signature of TPM_a and verifies whether the issuer which issues certificates is legal. If the issuer is legal and the DAA signature passes the verification, and TA-B obtains the signed certificate of domain A, TA-B will trust the publisher of domain A and verify the DAA signature of domain A.

Although ref. [15] uses a simple TA mechanism to solve the distrust problem among different trusted domains, it brings security risks while IssuerB issues certificates. As TPM uses different secret values for different publishers, TPM will use new secret value to generate the value comm which is signed with domain A's certificate. Then, TPM need to send the signature to IssuerB and the signed certificate to TA-B. Certainly, TA-B will verify domain A's signature instead of IssuerB. Though TA-B is able to verify whether comm is from a legal domain, it is impossible to confirm whether the platform that generates comm is the same as the one obtained from the signed certificate. In other words, it is impossible for TA-B to know whether the object, which it will issue certificate to, is the one that TA-A has verified. As $\text{Cert}_{\text{TA}-\text{A}}$ and the DAA signature of comm are separate and without any binding relationship, it is prone for a platform to steal $\text{Cert}_{\text{TA}-\text{A}}$ of another platform to apply domain B's DAA certificate. Finally, although ref. [13] proposes an inter-domain scheme, it is based on the agency signature and follows the RSA mechanism. It is low efficient.

We can see from above that no scheme has been proposed to realize a secure, practical and reliable inter-domain authentication for M2M networks. To achieve this goal, three problems should be considered. Firstly, the verifier of domain B should trust the DAA issuer of domain A. Secondly, after IssuerB succeeds the verification of domain A's local DAA signature, IssuerB can confirm the DAA certificate issuer and signed certificate are come from the same trusted platform. Thirdly, in the trusted platform, the secret values used to generate DAA certificates of domain A or domain B should not be the same. Those legacy inter-domain attestation algorithms are all based on the BCC-DAA scheme. According to the complex computation and low efficiency of BCC-DAA scheme, they are not fit for M2M devices and system at all. This paper designs a new M2M inter-domain attestation model at first. Then, based on this model, a new M2M lightweight inter-domain DAA (L-IDAA) scheme is proposed. Based on ECC-DAA scheme, the proposed L-IDAA not only meets the security needs and efficiency requirements, but also solves the three security problems mentioned above.

III. Proposed Inter-domain DAA Models

To simplify analysis, two DAA domains are presented as domain A and domain B respectively. Protocol entities in domain A include certificate issuer I_a, verifier V_a, host H_a and TPM_a. H_a and TPM_a make up the trusted platform P_a. Protocol entities in domain B include certificate issuer I_b, verifier V_b, host H_b and TPM_b, while H_b and TPM_b make up the trusted platform P_b.

Based on certificates hierarchy trust model, we design a lightweight inter-domain direct anonymous attestation model. A M2M Certification Authority (CA) system above different domains is proposed. The mutually authentication and communication between DAA systems from different domains are fulfilled by the unified management and interconnection of M2M CA system. The L-IDAA frameworks between two DAA domains are presented in Fig. 1.

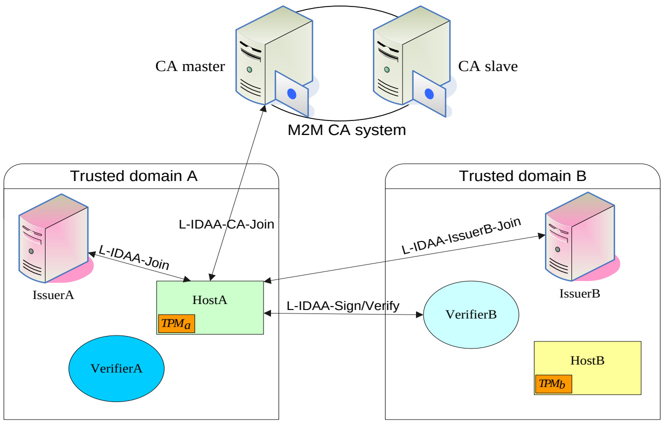

Fig.1 L-IDAA framework between two DAA domains

According to Fig. 1, L-IDAA adds three protocols in addition to single-domain DAA protocols: L-IDAA-CA-Join, L-IDAA-IssuerB-Join and L-IDAA-Sign/Verify. In L-IDAA-CA-Join protocol, CA issues a signed certificate $\text{Cert}_{\text{DAA}-\text{CA}}$ to the applier. In L-IDAA-IssuerB-Join protocol, with the signed certificate the trusted platform applies to IssuerB for DAA certificate $\text{Cert}_{\text{DAA}-\text{B}}$ of domain B. In L-IDAA-Sign/Verify protocol, the trusted platform in domain A takes advantage of $\text{Cert}_{\text{DAA}-\text{CA}}$ and $\text{Cert}_{\text{DAA}-\text{B}}$ to generate the DAA signature which is verified by verifier in domain B.

The process of L-IDAA can be described as follows. Legal issuer needs to register in CA and get public certificates issued by CA. CA stores and manages the public certificates of all legal publishers. H_a simultaneously obtains the DAA certificate and IssuerA's public key certificate from I_a, which are shown when the platform applies $\text{Cert}_\text{DAA-CA}$ from CA. Firstly, CA verifies the I_a public key certificate. After confirming its legality and credibility, CA uses the public key to verify the DAA signature issued by I_a. If the verification are passed, L-IDAA-CA-Join protocol is implemented, which means that CA issues the signed certificate $\text{Cert}_\text{DAA-CA}$ to H_a.

H_a needs to prove two points to CA. One is that H_a has the DAA certificate Cert_DAA issued by I_a; the other one is that the secret value for applying the signed certificate conforms to that for Cert_DAA. Then, H_a uses the signed certificate to apply for the DAA certificate in domain B, which is the implementation of L-IDAA-IssuerB-Join protocol. H_{a} needs to prove the possession of the signed certificate issued by CA, and confirms that the secret value it provides to I_{b} and the signed certificate are owned by the same platform. Only with the two certificates at the same time, it is possible to generate the inter-domain DAA signature so that it can confirm platform's authenticity to verifiers of different domains.

IV. The Proposed Inter-domain Anonymous Attestation Scheme—L-IDAA

A. L-IDAA-CA-Join Protocol

The protocol is implemented after the trusted platform in domain A fulfills L-IDAA-join protocol and obtains the DAA certificate issued by IssuerA. If the trusted platform needs to communicate with verifiers in other domains, it is necessary to first get the signed certificate $\mathrm{Cert}_{\mathrm{DAA-CA}}$ issued by CA.

The public parameters of CA system are($G_{\mathrm{CA}_1}, G_{\mathrm{CA}_2}, G_{\mathrm{CA}_\mathrm{T}}, \hat{t}, P_{\mathrm{CA}_1}, P_{\mathrm{CA}_2}, P_{\mathrm{CA}_3}, P_{\mathrm{CA}_4}, q, H_1, X_{\mathrm{CA}}, Y_{\mathrm{CA}}$. Here,$G_{\mathrm{CA}_1} = \langle P_{\mathrm{CA}_1} \rangle$, $G_{\mathrm{CA}_2} = \langle P_{\mathrm{CA}_2} \rangle$, $\hat{t}: G_{\mathrm{CA}_1} \times G_{\mathrm{CA}_2} \mapsto G_{\mathrm{CA}_\mathrm{T}}$, $H_1: \{0,1\}^* \mapsto Z_\mathrm{q}$. X_{CA} and Y_{CA} are the public keys of CA, x_{CA} and y_{CA} are the secret keys respectively. $X_{\mathrm{CA}} = x_{\mathrm{CA}} P_{\mathrm{CA}_2} \in G_{\mathrm{CA}_2}$, $Y_{\mathrm{CA}} = y_{\mathrm{CA}} P_{\mathrm{CA}_2} \in G_{\mathrm{CA}_2}$.

Assume that the $\mathrm{Cert}_{\mathrm{DAA-CA}}$ of domain A is (A,B,C,D). The protocol process that P_{a} gets the signed certificate $\mathrm{Cert}_{\mathrm{DAA-CA}}$ is described as follows.

1. CA chooses and sends a random number $n_{\mathrm{CA}} \leftarrow \{0,1\}^{\mathrm{t}}$ to H_{a} , which is a host in domain A.
2. H_{a} randomly chooses $l \leftarrow Z_\mathrm{q}$ and computes $R \leftarrow [l]A$; $S \leftarrow [l]B$; $T \leftarrow [l]C$; $W \leftarrow [l]D$, while $h = \mathrm{H}(R \| S \| T \| W \| n_{\mathrm{CA}})$. Then H_{a} sends h to $\mathrm{TPM}_{\mathrm{a}}$.
3. $\mathrm{TPM}_{\mathrm{a}}$ generates secret value f and computes $Q_{\mathrm{CA}} = [f]P_{\mathrm{CA}_1} + [\mathrm{Ident}]P_{\mathrm{CA}_3}$, Ident=H($\mathrm{EK}_{\mathrm{pub}}$ ||TRE_id||n_{id}). Here, the Ident is the identity of the platform, $\mathrm{EK}_{\mathrm{pub}}$ is the public key part of EK, TRE_id is the ID number of the trusted platform and n_{id} is the random number TPM chooses.
4. $\mathrm{TPM}_{\mathrm{a}}$ runs Zero-knowledge proof protocol: $\mathrm{PK}\{(f, \mathrm{Ident}): Q_{\mathrm{CA}} = [f]P_{\mathrm{CA}_1} + [\mathrm{Ident}]P_{\mathrm{CA}_3} \wedge W = [f]S\}$. Then TPM chooses $r_\mathrm{f}, r_{\mathrm{Ident}} \leftarrow Z_\mathrm{q}$, $n_\mathrm{T} \leftarrow \{0,1\}^{\mathrm{t}}$ and computes $U = [r_\mathrm{f}]S$, $V_{\mathrm{CA}} = [r_\mathrm{f}]P_{\mathrm{CA}_1} + [r_{\mathrm{Ident}}]P_{\mathrm{CA}_3}$, $c = \mathrm{H}(h || P_{\mathrm{CA}_1} \| P_{\mathrm{CA}_3} \| U \| V_{\mathrm{CA}} \| Q_{\mathrm{CA}} || n_\mathrm{T})$, $s_\mathrm{f} = r_\mathrm{f} + c \cdot f$, $s_{\mathrm{Ident}} = r_{\mathrm{Ident}} + c \cdot \mathrm{Ident}$. Then $\mathrm{TPM}_{\mathrm{a}}$ sends $(Q_{\mathrm{CA}}, c, s_\mathrm{f}, s_{\mathrm{Ident}}, n_\mathrm{T})$ to H_{a} and H_{a} sends （$R,S,T,W,Q_{\mathrm{CA}},c, s_\mathrm{f}, s_{\mathrm{Ident}}, n_\mathrm{T}, n_{\mathrm{CA}}$） to the CA. Here, $\mathrm{TPM}_{\mathrm{a}}$ uses Zero-knowledge proof to prove that (a) TPM has the certificate $\mathrm{Cert}_{\mathrm{DAA-A}}$ (A,B,C,D) issued by IssuerA, and (b) the value f used to get certificate issued by CA is the same as the f used in $\mathrm{Cert}_{\mathrm{DAA-A}}$.
5. The CA issuer makes verifications as follows.
   1) Firstly, it makes a counterfeit verification and examine whether W is equal to $[f]S$ according to the known counterfeit value f.
   2) It makes a correctness verification of the parameters R, S, T and W of DAA certificate in domain A. Then it does the examination whether the formulas below are the same. $\hat{t}(R, Y_{\mathrm{CA}})? = \hat{t}(S, P_{\mathrm{CA}_2}), \hat{t}(R + W, X_{\mathrm{CA}})? = \hat{t}(T, P_{\mathrm{CA}_2})$.
   3) Finally, CA issuer verifies the secret value f and Zero-knowledge proof of DAA certificate in domain A so as to confirm that the secret value f used to generate Q_{CA} by $\mathrm{TPM}_{\mathrm{a}}$ is the same as the counterpart of DAA certificate in domain A.

Here, the CA issuer also calculates the formulas: $U' = [s_\mathrm{f}]S - [c]W$, $V'_{\mathrm{CA}} = [s_\mathrm{f}]P_{\mathrm{CA}_1} + [s_{\mathrm{Ident}}]P_{\mathrm{CA}_3} - [c]Q_{\mathrm{CA}}$ and verifies whether c is equal to $\mathrm{H}(\mathrm{H}(R \| S \| T \| W \| n_{\mathrm{CA}}) || P_{\mathrm{CA}_1} \| P_{\mathrm{CA}_3} \| U' \| V'_{\mathrm{CA}} \| Q_{\mathrm{CA}} || n_\mathrm{T})$.

If CA fulfills the verification, it will make a signature and issue a signed certificate $\mathrm{Cert}_{\mathrm{DAA-CA}}$ to the trusted platform P_{a}. The signed certificate $\mathrm{Cert}_{\mathrm{DAA-CA}}$ is encoded as follows. Assume that the issuer's name is $\mathrm{CA}_{\mathrm{name}} \in \{0,1\}^{\mathrm{t}}$, and the certificate effective date is $\mathrm{CA}_{\mathrm{date}} \in \{0,1\}^{\mathrm{t}}$. CA chooses $r \leftarrow Z_\mathrm{q}$ and calculates the following formulas.

$A_{\mathrm{CA}} = [r]P_{\mathrm{CA}_1}, B_{\mathrm{CA}} = [y_{\mathrm{CA}}]A_{\mathrm{CA}}, E_{\mathrm{CA}} = [r]P_{\mathrm{CA}_3}, F_{\mathrm{CA}} = [y_{\mathrm{CA}}]E_{\mathrm{CA}}$,

$G_{\mathrm{CA}} = [r]P_{\mathrm{CA}_4}; H_{\mathrm{CA}} = [y_{\mathrm{CA}}]G_{\mathrm{CA}}$, $D_{\mathrm{CA}} = [f]B_{\mathrm{CA}} + [\mathrm{Ident}]F_{\mathrm{CA}} + [\mathrm{CA}_{\mathrm{date}} || \mathrm{CA}_{\mathrm{name}}]H_{\mathrm{CA}}$, $C_{\mathrm{CA}} = [x_{\mathrm{CA}}](A_{\mathrm{CA}} + D_{\mathrm{CA}})$.

Here, $(A_{\mathrm{CA}}, B_{\mathrm{CA}}, C_{\mathrm{CA}}, D_{\mathrm{CA}}, E_{\mathrm{CA}}, F_{\mathrm{CA}}, G_{\mathrm{CA}}, H_{\mathrm{CA}}, \mathrm{CA}_{\mathrm{date}}, \mathrm{CA}_{\mathrm{name}})$ is the CL-LRSW signature of (f, Ident, $\mathrm{CA}_{\mathrm{name}}, \mathrm{CA}_{\mathrm{date}}$). It is named as the signed certificate $\mathrm{Cert}_{\mathrm{DAA-CA}}$ issued by CA.

B. L-IDAA-IssuerB-Join Protocol

This is an inter-domain protocol implemented between the trusted platform P_{a} in domain A and certificate issuer I_{b} in domain B. Based on this protocol, P_{a} gets the DAA certificate of domain B with which P_{a} is able to sign/verify with verifier in domain B.

The public parameters of IssuerB system are described as $(G_{\mathrm{IB}_1}, G_{\mathrm{IB}_2}, G_{\mathrm{IB}_\mathrm{T}}, \hat{t}, P_{\mathrm{IB}_1}, P_{\mathrm{IB}_2}, P_{\mathrm{IB}_3}, P_{\mathrm{IB}_4}, q, H_1, X_{\mathrm{IB}}, Y_{\mathrm{IB}})$. Here, $G_{\mathrm{IB}_1} = \langle P_{\mathrm{IB}_1} \rangle$, $G_{\mathrm{IB}_2} = \langle P_{\mathrm{IB}_2} \rangle$, $\hat{t}: G_{\mathrm{IB}_1} \times G_{\mathrm{IB}_2} \mapsto G_{\mathrm{IB}_\mathrm{T}}$. X_{IB} and Y_{IB} are the public keys of IssuerB, x_{IB} and y_{IB} are the secret keys. $X_{\mathrm{IB}} = x_{\mathrm{IB}} P_{\mathrm{IB}_2} \in G_{\mathrm{IB}_2}$, $Y_{\mathrm{IB}} = y_{\mathrm{IB}} P_{\mathrm{IB}_2} \in G_{\mathrm{IB}_2}$.

Now the trusted platform P_{a} has owned the DAA certificate of domain A as $\mathrm{Cert}_{\mathrm{DAA-A}}$ and the signed certificate issued by CA is $\mathrm{Cert}_{\mathrm{DAA-CA}}$. Because the secret value f have been used in application for $\mathrm{Cert}_{\mathrm{DAA-A}}$, the next secret value k should be used in application for $\mathrm{Cert}_{\mathrm{DAA-B}}$.

The L-IDAA-IssuerB-Join protocol is described as follows.

1. IssuerB I_{B} chooses a random number $n_{\mathrm{IB}} \leftarrow \{0,1\}^{\mathrm{t}}$ and sends it to HostA H_{a}.
2. H_{a} generates a secret value k and calculates $Q_{\mathrm{IB}} = [k]P_{\mathrm{IB}_1} + [\mathrm{Ident}]P_{\mathrm{IB}_3}$. Then it chooses a random number $j \leftarrow Z_\mathrm{q}$ and computes the followings.

$R_{\mathrm{CA}} \leftarrow [j]A_{\mathrm{CA}}, S_{\mathrm{CA}} = [j]B_{\mathrm{CA}}, T_{\mathrm{CA}} = [j]C_{\mathrm{CA}}, W_{\mathrm{CA}} = [j]D_{\mathrm{CA}}$

$K_{\mathrm{CA}} = [j]E_{\mathrm{CA}}, \quad L_{\mathrm{CA}} = [j]F_{\mathrm{CA}}, \quad M_{\mathrm{CA}} = [j]G_{\mathrm{CA}}, \quad N_{\mathrm{CA}} = [j]H_{\mathrm{CA}}$

$\mathrm{str} \leftarrow R_{\mathrm{CA}} \| S_{\mathrm{CA}} \| T_{\mathrm{CA}} \| W_{\mathrm{CA}} \| K_{\mathrm{CA}} \| L_{\mathrm{CA}} \| M_{\mathrm{CA}} \| N_{\mathrm{CA}} \| Q_{\mathrm{IB}}$.

3. The trusted platform P_{a}makes Zero-knowledge proof on *f*, *k* and Ident as

$$\mathrm{PK}\left\{\begin{array}{c}(f, \mathrm{Ident}, k): \\ Q_{\mathrm{IB}} = [k]P_{\mathrm{IB}_1} + [\mathrm{Ident}]P_{\mathrm{IB}_3} \land W_{\mathrm{CA}} = [f]S_{\mathrm{CA}} + [\mathrm{Ident}] \\ L_{\mathrm{CA}} + [\mathrm{CA}_{\mathrm{date}} \| \mathrm{CA}_{\mathrm{name}} \| N_{\mathrm{CA}}]\end{array}\right\}.$$

Here, the Zero-knowledge proof is to confirm that: (a) $(\mathrm{TPM}_{\mathrm{a}}, H_{\mathrm{a}})$ has the certificate $\mathrm{Cert}_{\mathrm{DAA-CA}}$ issued by CA; (b) the Ident used to generate Q_{IB} of $\mathrm{Cert}_{\mathrm{DAA-B}}$ is the same as Ident in $\mathrm{Cert}_{\mathrm{DAA-CA}}$. If they are the same, it means that the appliers for the two certificates are come from the same trusted platform.

The Zero-knowledge proof is working as follows.

(1) H_{a} chooses $r_{\mathrm{Ident}}, r_{\mathrm{k}} \leftarrow Z_{\mathrm{q}}$ and computes $V_{\mathrm{IB}} = [r_{\mathrm{k}}]P_{\mathrm{IB}_1} + [r_{\mathrm{Ident}}]P_{\mathrm{IB}_3}$, $h = \mathrm{H}(\mathrm{str} \| V_{IB} \| n_{\mathrm{IB}})$. Then it send *h*, $r_{\mathrm{Ident}}, r_{\mathrm{k}}$ and the secret value *k* to $\mathrm{TPM}_{\mathrm{a}}$.

(2) $\mathrm{TPM}_{\mathrm{a}}$ chooses $r_{\mathrm{f}} \leftarrow Z_{\mathrm{q}}, n_{\mathrm{T}} \leftarrow \{0,1\}^{\mathrm{t}}$ and calculates $U_{\mathrm{CA}} = [r_{\mathrm{f}}]S_{\mathrm{CA}} + [r_{\mathrm{Ident}}]L_{\mathrm{CA}}$, $c = \mathrm{H}(h || P_{\mathrm{IB}_1} \| P_{\mathrm{IB}_3} \| U_{\mathrm{CA}} || n_{\mathrm{T}})$, $s_{\mathrm{f}} = r_{\mathrm{f}} + c \cdot f$, $s_{\mathrm{Ident}} = r_{\mathrm{Ident}} + c \cdot \mathrm{Ident}$, $s_{\mathrm{k}} = r_{\mathrm{k}} + c \cdot k$.Then, it sends c, s_{f}, $s_{\mathrm{Ident}}, s_{\mathrm{k}}, n_{\mathrm{T}}$ to H_{a}.

Here, in the processing of Q_{IB} signature, we can see that any computation relevant to *f* is only implemented by $\mathrm{TPM}_{\mathrm{a}}$. The reason is that *f* is only known by $\mathrm{TPM}_{\mathrm{a}}$ and secret to HostA. As $\mathrm{TPM}_{\mathrm{a}}$ and HostA share *k* and Ident, they can fulfill computation requirement according to *k* and Ident.

(3) H_{a} sends its verification information ($R_{\mathrm{CA}}, S_{\mathrm{CA}}, T_{\mathrm{CA}}, W_{\mathrm{CA}}, K_{\mathrm{CA}}, L_{\mathrm{CA}}, M_{\mathrm{CA}}, N_{\mathrm{CA}}, Q_{\mathrm{IB}}$, c,$s_{\mathrm{f}}, s_{\mathrm{k}}, s_{\mathrm{Ident}}, n_{\mathrm{T}}, n_{\mathrm{CA}}$) to IssuerB.

(4) The IssuerB in domain B verifies HostA as follows.

Firstly it computes $U'_{\mathrm{CA}} = [s_{\mathrm{f}}]S_{\mathrm{CA}} + [s_{\mathrm{Ident}}]L_{\mathrm{CA}} - [c](W_{\mathrm{CA}} - [\mathrm{CA}_{\mathrm{date}} || \mathrm{CA}_{\mathrm{name}}]N_{\mathrm{CA}})$, $V'_{\mathrm{IB}} = [s_{\mathrm{k}}]P_{\mathrm{IB}_1} + [s_{\mathrm{Ident}}]P_{\mathrm{IB}_3} - [c]Q_{\mathrm{IB}}$,

$\mathrm{str}' \leftarrow R_{\mathrm{CA}} \| S_{\mathrm{CA}} \| T_{\mathrm{CA}} \| W_{\mathrm{CA}} \| K_{\mathrm{CA}} \| L_{\mathrm{CA}} \| M_{\mathrm{CA}} \| N_{\mathrm{CA}} \| Q_{\mathrm{IB}}$, $h' = \mathrm{H}(\mathrm{str}' \| V'_{\mathrm{IB}} \| n_{\mathrm{IB}})$.

Then it verifies whether c is equal to $\mathrm{H}(h' || P_{\mathrm{IB}_1} \| P_{\mathrm{IB}_3} \| U'_{\mathrm{CA}} || n_{\mathrm{T}})$.

If IssuerB fulfills the verification, IssuerB issues the DAA certificate of domain B to P_{a}, which includes the following information: the issuer's name $\mathrm{IB}_{\mathrm{name}} \in \{0,1\}^{\mathrm{t}}$, and the certificate's effective date $\mathrm{IB}_{\mathrm{date}} \in \{0,1\}^{\mathrm{t}}$. Then, CA chooses $r \leftarrow Z_{\mathrm{q}}$ and calculates the following formulas.

$A_{\mathrm{IB}} = [r]\, P_{\mathrm{IB}_1}$, $B_{\mathrm{IB}} = [y_{\mathrm{IB}}]A_{\mathrm{IB}}$, $E_{\mathrm{IB}} = [r]P_{\mathrm{IB}_3}$, $F_{\mathrm{IB}} = [y_{\mathrm{IB}}]E_{\mathrm{IB}}, G_{\mathrm{IB}} = [r]P_{\mathrm{IB}_4}, H_{\mathrm{IB}} = [y_{\mathrm{IB}}]G_{\mathrm{IB}}$,

$D_{\mathrm{IB}} =[\, y_{\mathrm{IB}} \cdot r\,](\, Q_{\mathrm{IB}} + [\mathrm{IB}_{\mathrm{date}} || \mathrm{IB}_{\mathrm{name}}]P_{\mathrm{IB}_4}) = [k]B_{\mathrm{IB}} + [\mathrm{Ident}]F_{\mathrm{IB}} + [\mathrm{IB}_{\mathrm{date}} || \mathrm{IB}_{\mathrm{name}}]H_{\mathrm{IB}}$, $C_{\mathrm{IB}} = [x_{\mathrm{IB}}](A_{\mathrm{IB}} + D_{\mathrm{IB}})$.

Here, $(A_{\mathrm{IB}}, B_{\mathrm{IB}}, C_{\mathrm{IB}}, D_{\mathrm{IB}}, E_{\mathrm{IB}}, F_{\mathrm{IB}}, G_{\mathrm{IB}}, H_{\mathrm{IB}})$ is the CL-LRSW signature of（k, Ident, $\mathrm{IB}_{\mathrm{name}}, \mathrm{IB}_{\mathrm{date}}$）, and is named as the DAA certificate $\mathrm{Cert}_{\mathrm{DAA-B}}$.

C. L-IDAA-Sign/Verify Protocol

This also is an inter-domain sign/verify protocol run between the trusted platform P_{a} in domain A and verifier in domain B. P_{a} makes an inter-domain signature with L-IDAA-Sign and then sends the signature to verifierB V_{b} that will make an IDAA/Verify operation. Only passing the verification can P_{a} anonymously confirm its credibility to verifiers in different domains.

The trusted platform must own the signed certificate $\mathrm{Cert}_{\mathrm{DAA-CA}}$ issued by CA and the DAA certificate in domain B $\mathrm{Cert}_{\mathrm{DAA-B}}$ at the same time.

The L-IDAA/Sign process are described as follows.

1. VeriferB sends H_{a} a random number $n_{\mathrm{IB}} \in \{0,1\}^{\mathrm{t}}$ and a base name $\mathrm{bsn}_{\mathrm{IB}}$.
2. HostA H_{a} randomly chooses $l_{\mathrm{CA}} \leftarrow Z_{\mathrm{q}}, j_{\mathrm{IB}} \leftarrow Z_{\mathrm{q}}$ and makes the following calculations.

$A'_{\mathrm{CA}} = [l_{CA}]A_{\mathrm{CA}}, B'_{\mathrm{CA}} = [l_{CA}]B_{\mathrm{CA}}, C'_{\mathrm{CA}} = [l_{CA}]C_{\mathrm{CA}}, D'_{\mathrm{CA}} = [l_{CA}]D_{\mathrm{CA}}$,

$E'_{\mathrm{CA}} = [l_{CA}]E_{\mathrm{CA}}, F'_{\mathrm{CA}} = [l_{CA}]F_{\mathrm{CA}}, G'_{\mathrm{CA}} = [l_{CA}]G_{\mathrm{CA}}$, $H'_{\mathrm{CA}} = [l_{CA}]H_{\mathrm{CA}}$,

$A'_{\mathrm{IB}} = [j_{IB}]A_{\mathrm{IB}}, B'_{\mathrm{IB}} = [j_{IB}]B_{\mathrm{IB}}, C'_{\mathrm{IB}} = [j_{IB}]C_{\mathrm{IB}}$, $D'_{\mathrm{IB}} = [j_{IB}]D_{\mathrm{IB}}$,

$E'_{\mathrm{IB}} = [j_{IB}]E_{\mathrm{IB}}$, $F'_{\mathrm{IB}} = [j_{IB}]F_{\mathrm{IB}}$, $G'_{\mathrm{IB}} = [j_{IB}]G_{\mathrm{IB}}$, $H'_{\mathrm{IB}} = [j_{IB}]H_{\mathrm{IB}}$,

Then HostA chooses $r_{\mathrm{Ident}}, r_{\mathrm{k}} \leftarrow Z_{\mathrm{q}}$ and computes

$U_{\mathrm{IB}} = [r_{\mathrm{k}}]B'_{\mathrm{IB}} + [r_{\mathrm{Ident}}]F'_{\mathrm{IB}}$,

$\mathrm{str1} \leftarrow A'_{\mathrm{CA}} \| B'_{\mathrm{CA}} \| C'_{\mathrm{CA}} \| D'_{\mathrm{CA}} \| E'_{\mathrm{CA}} \| F'_{\mathrm{CA}} \| G'_{\mathrm{CA}} \| H'_{\mathrm{CA}}$,

$\mathrm{str2} \leftarrow A'_{\mathrm{IB}} \| B'_{\mathrm{IB}} \| C'_{\mathrm{IB}} \| D'_{\mathrm{IB}} \| E'_{\mathrm{IB}} \| F'_{\mathrm{IB}} \| G'_{\mathrm{IB}} \| H'_{\mathrm{IB}}$,

$h = \mathrm{H}(\mathrm{str1} \| \mathrm{str2} \| n_{\mathrm{IB}} \| U_{\mathrm{IB}})$.

Finally, H_{a} sends *h*, $\mathrm{bsn}_{\mathrm{IB}}$ and r_{Ident} to $\mathrm{TPM}_{\mathrm{a}}$.

3. $\mathrm{TPM}_{\mathrm{a}}$ makes signature on msg as following. It firstly chooses $r_{\mathrm{f}} \leftarrow Z_{\mathrm{q}}$ and computes $U_{\mathrm{CA}} = [r_{\mathrm{f}}]B'_{\mathrm{CA}} + [r_{\mathrm{Ident}}]F'_{\mathrm{CA}}$,

$c = \mathrm{H}(h \| P_{\mathrm{CA}_1} \| P_{\mathrm{CA}_3} \| P_{\mathrm{IB}_1} \| P_{\mathrm{IB}_3} \| U_{\mathrm{CA}} \| n_{\mathrm{T}} || \mathrm{bsn}_{\mathrm{IB}} \| \mathrm{msg})$, $s_{\mathrm{f}} = r_{\mathrm{f}} + c \cdot f, s_{\mathrm{Ident}} = r_{\mathrm{Ident}} + c \cdot \mathrm{Ident}$, $s_{\mathrm{k}} = r_{\mathrm{k}} + c \cdot k$.

Then, TPM sends $c, s_{\mathrm{f}}, s_{\mathrm{Ident}}, s_{\mathrm{k}}$ and n_{T} to Host, which gets the inter-domain signature σ_{AB} as ($A'_{\mathrm{CA}}, B'_{\mathrm{CA}}, C'_{\mathrm{CA}}, D'_{\mathrm{CA}}, E'_{\mathrm{CA}}, F'_{\mathrm{CA}}, G'_{\mathrm{CA}}, H'_{\mathrm{CA}}, A'_{\mathrm{IB}}, B'_{\mathrm{IB}}, C'_{\mathrm{IB}}$, $D'_{\mathrm{IB}}, E'_{\mathrm{IB}}, F'_{\mathrm{IB}}, G'_{\mathrm{IB}}, H'_{\mathrm{IB}}, c, s_{\mathrm{f}}, s_{\mathrm{Ident}}, s_{\mathrm{k}}, n_{\mathrm{T}}$)

Here, the Zero-knowledge signature can prove that: (a) TPM/Host owns the certificate $\mathrm{Cert}_{\mathrm{DAA-CA}}$ issued by CA and the certificate $\mathrm{Cert}_{\mathrm{DAA-B}}$ issued by IssuerB; (b) The two certificates are come from the same platform and is bound by parameter Ident; (c) TPM must be used in the calculation of inter-domain DAA signature since the secret *f* stored in TPM.

Finally, the processing of L-IDAA/Verify is described as follows.

1. The verifier computes

$\mathrm{str1} \leftarrow A'_{\mathrm{CA}} \| B'_{\mathrm{CA}} \| C'_{\mathrm{CA}} \| D'_{\mathrm{CA}} \| E'_{\mathrm{CA}} \| F'_{\mathrm{CA}} \| G'_{\mathrm{CA}} \| H'_{\mathrm{CA}}$,

$\mathrm{str2} \leftarrow A'_{\mathrm{IB}} \| B'_{\mathrm{IB}} \| C'_{\mathrm{IB}} \| D'_{\mathrm{IB}} \| E'_{\mathrm{IB}} \| F'_{\mathrm{IB}} \| G'_{\mathrm{IB}} \| H'_{\mathrm{IB}}$,

$U'_{\mathrm{CA}} = [s_{\mathrm{f}}]B'_{\mathrm{CA}} + [s_{\mathrm{Ident}}]F'_{\mathrm{CA}} - c \cdot (D'_{\mathrm{CA}} - [\mathrm{CA}_{\mathrm{date}} || \mathrm{CA}_{\mathrm{name}}]H'_{\mathrm{CA}})$,

$$U_{\mathrm{IB}}' = [s_{\mathrm{k}}]B_{\mathrm{IB}}' + [s_{\mathrm{Ident}}]F_{\mathrm{IB}}' - c \cdot (D_{\mathrm{IB}}' - [\mathrm{IB}_{\mathrm{date}} || \mathrm{IB}_{\mathrm{name}}]H_{\mathrm{IB}}').$$

2. Then, it verifies whether c is equal to $\mathrm{H}(\mathrm{H}(\mathrm{str1} \| \mathrm{str2} \| n_{\mathrm{IB}} \| U_{\mathrm{IB}}') \| P_{\mathrm{CA}_1} \| P_{\mathrm{CA}_3} \| P_{\mathrm{IB}_1} \| P_{\mathrm{IB}_3} \| U_{\mathrm{CA}}' \| n_{\mathrm{T}} || \mathrm{bsn}_{\mathrm{IB}} \| \mathrm{msg})$.

V. Analysis of the Proposed L-IDAA Scheme

A. Security Analysis of L-IDAA

As the L-IDAA scheme is constructed based on the single-domain DAA scheme [10], its security is mainly the same as the security of single-domain DAA scheme. In L-IDAA scheme, there are two join processes. The one is L-IDAA-CA-Join and the other is L-IDAA-IssuerB-Join. All these two join processes do the same works as the sign process in the single-domain DAA scheme specified in ref. [10]. Consequently, this paper mainly analyzes the security of L-IDAA-Sign/Verify protocol.

Here, the security of L-IDAA-Sign/Verify protocol mainly lies in the unforgeability and anonymity.

Unforgeability:

(1) Valid TPM must be used in the inter-domain signature. Because an inter-domain signature requires the secret value *f*, it is only known by TPM in the entire process and any other entity including Host can't get this value.

(2) In order to make a valid inter-domain signature, the trusted platform must obtain the signed certificate and DAA certificate in domain B. Lack of anyone will result in the failure of the inter-domain attestation.

We can find out from section IV that the L-IDAA scheme have fully realized the above two point, the unforgeability of L-IDAA scheme is proved.

Anonymity:

The EK of one platform is always stored in the TPM model of this platform. TPM need present local IssuerA with EK to show its valid identity only when getting the DAA certificates in domain A. To get other certificates, there is no need to present its own EK. In the application for the signed certificate $\mathrm{Cert}_{\mathrm{DAA-CA}}$ issued by CA, the applier only needs to confirm the possession of legal $\mathrm{Cert}_{\mathrm{DAA-A}}$. In the application for the certificate in domain B, the applier only needs to prove the possession of $\mathrm{Cert}_{\mathrm{DAA-CA}}$ to IssuerB. Therefore, there is no need to show EK when getting certificates in the L-IDAA-CA-Join process and L-IDAA-IssuerB-Join process. Therefore, compared with the anonymity of single-domain DAA, the anonymity of the inter-domain attestation L-IDAA scheme is ensured.

B. Efficiency Analysis of L-IDAA

According to the inter-domain DAA scheme (BCC-IDAA) proposed by Xiaofeng Chen [8], we compare the protocol performance of the proposed L-IDAA scheme with BCC-IDAA. Here, we mainly compare the computational cost of TPM and Host in the processes of certificate application and certificate signing, which are shown in Table 1.

Table 1 performance comparison between two inter-domain DAA schemes

Scheme	Period	TPM	Host
BCC-IDAA	IDAA-IssuePassport	$3G_{\mathrm{N}}^3$+$2G_{\Gamma}$	$3G_{\mathrm{N}} + 1G_{\mathrm{N}}^2 + 2G_{\mathrm{N}}^3 + 1G_{\mathrm{N}}^4$
	IDAA-IssueVisa	G_{N}^3+$2G_{\Gamma}$	$G_{\mathrm{N}} + 2G_{\mathrm{N}}^3 + 3G_{\mathrm{N}}^4 + 1G_{\mathrm{N}}^5$
	IDAA-Sign/Verify	G_{N}^3+G_{Γ}	$2G_{\mathrm{N}} + 4G_{\mathrm{N}}^3 + 2G_{\mathrm{N}}^4 + 1G_{\mathrm{N}}^5 + 1G_{\mathrm{N}}^9$
L-IDAA	L-IDAA-CA-Join	$1G_1$+2 G_1^2	$4G_1$
	L-IDAA-IssuerB-Join	$1G_1^2$	$8G_1$+$2G_1^2$
	L-IDAA-Sign/Verify	$1G_1^2$	$16G_1$+$1G_1^2$

According to the performance analysis method in ref. [4], it is found that the computational costs of each protocols in the proposed L-IDAA scheme is lower than those in BCC-IDAA scheme no matter in the process of obtaining certificates or in the process of signing or verifying. Since the L-IDAA-Sign/Verify protocol functioned frequently, the computational costs of TPM and Host are $1G_1^2$ and $16G_1$+$1G_1^2$ respectively, which are computed in group G_1 and the computational costs are low. However, for TPM or Host in BCC-IDAA scheme, the computational costs are larger and many computations of complex exponents $G_{\mathrm{j}}^{\mathrm{m}}\{j=\mathrm{N}, \Gamma\}$ are needed.

Moreover, the BCC-IDAA verification requires a large number of Zero-knowledge proofs, and the verification process is too complex to implement. However, the proposed L-IDAA scheme not only has simple protocols and low computational costs, but also solves several secure problems such as distrust among different domains and incompletion of bounding several certificates to the same platform. As a result, the proposed L-IDAA scheme can provide security to platform anonymity attestation among different trusted domains in M2M networks.

VI. Conclusion

According to the features of M2M networks, a M2M inter-domain platform attestation model and an attestation scheme L-IDAA based on the model are proposed. The security proof and efficiency analysis of L-IDAA scheme are given and shown that the L-IDAA scheme is secure and efficient. Since the proposed scheme can fit the security fault of those legacy inter-domain schemes and has low computational cost and high efficiency, it provides a solution for M2M inter-domain platform attestation and ensures the security for wider applications of M2M networks.

ACKNOWLEDGMENT

This work was supported in part by the national High Technology Research and Development Program of China (863 program) under grant No. 2013AA014001 and by the national Natural Science Foundation of China (NSFC) under grant No.61372103.

REFERENCES

[1] E. Brickell, J. Camenisch, L. Chen, “Direct anonymous attestation”, the 11th ACM Conference on Computer and Communications Security, 2004, pp. 132–145.

[2] L. Chen, P. Morrissey, N. P. Smart, “Fixing the pairing based protocols”, Cryptology ePrint Archive, Report 2009/198, http://eprint.iacr.org/2009 /198.

[3] S. Lien, K. Chen, “Toward Ubiquitous Massive Accesses in 3GPP Machine-to-Machine Communications,” IEEE Communications Magazine, Vol. 30(4), pp. 66–74, 2011.

[4] C. Hongsong, “Security and Trust Research in M2M networks,” IEEE Communications Magazine, Vol. 34(6), pp. 286–290, 2011.

[5] M. Beale, “Future challenges in efficiently supporting M2M in the LTE standards,” 2012 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), pp. 186–190, Apr. 2012.

[6] I. Cha, Y. Shah, A. U. Schmidt, A. Leicher, “Trust in M2M,” IEEE cehicular technology magazine, Vol. 56(5), pp. 69–75, 2009.

[7] R. Lu, X. Li, X. Liang, X. S. Shen, “GRS: The Green, Reliability, and Security of Emerging Machine to Machine Communications,” IEEE Communications Magazine, Vol. 31(5), pp. 28–35, 2011.

[8] X. Chen, D. Feng. “Direct anonymous attestation for next generation TPM”. Journal of Computers, Vol. 31(7), pp.1122-1129. 2008.

[9] L. Chen, D. Page, N. P. Smart, “On the design and implementation of an efficient DAA scheme”, CARDIS 2010. LNCS, Vol.6035, pp.223-238.

[10] Liqun Chen, “A DAA Scheme Using Batch Proof and Verification”, TRUST 2010, LNCS, Vol. 6101, pp.166-180.

[11] E. Brickell, L. Chen, J. Li, “A new direct anonymous attestation scheme from bilinear maps”, TRUST 2008, Springer-Verlag LNCS, Vol. 4968, pp. 166-178, 2008.

[12] E. Brickell, J. Li, “Enhanced privacy ID: A direct anonymous attestation scheme with enhanced revocation capabilities”, the 6th ACM Workshop on Privacy in the Electronic Society (WPES 2007). ACM Press, pp. 21-30, 2007.

[13] L. Yang, J. Ma, Q. Jiang, “Direct anonymous attestation scheme in cross trusted domain for wireless mobile networks”, Journal of software, Vol. 23(5), pp. 1260-1271, 2012.

[14] Y. Yang, L. Cao, Z. Li, “A Novel Direct Anonymous Attestation Protocol Based on Zero Knowledge Proof for Different Trusted Domains”, China Communications, Vol. 41(3), pp.54-61, 2010.

[15] L. Sun, G. Chang, “A Strict Inter-Domain Anonymity Attestation Scheme”, Computer Design and Applications, Vol. 45, pp.31-36, 2010.