Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2007, Article ID 56050, 7 pages
doi:10.1155/2007/56050

Research Article

Mobile Broadcast DRM Based on User Identity Card

Byung-Rae Lee

Telecommunication R&D Center, Samsung Electronics, Suwon-si, Gyenggi-do 443-742, South Korea

Received 10 December 2006; Revised 22 July 2007; Accepted 12 August 2007

Recommended by Kameswara Rao Namuduri

The current mobile broadcast systems do not provide efficient solution for consumption of service and content based on the user identity card such as a smartcard. This prevents users from consuming broadcast service and contents independent of a specific terminal (e.g., the one used for registration or purchase). To provide usage of broadcast services based on the user identity card, mutual authentication needs to be established among the service provider, the terminal, and the user identity card whenever the terminal is changed. The crucial element for this is assuring the service provider, the terminal, and the user identity card by authenticating each entity to the other entities. In this paper, we propose the new authentication scheme, which provides efficient scheme for three kinds of mutual authentications among the service provider, the terminal, and the user identity card. We also construct mobile broadcast DRM system based on the proposed authentication scheme for consumption of broadcast services with multiple terminals.

1. INTRODUCTION

Digital rights management (DRM) is widely recognized as an important tool for managing contents around wireless or wired network. Recently, DRM has extended its area to mobile broadcast systems such as DVB-H [1] and open mobile alliance (OMA) BCAST [2, 3]. DRM profile in OMA BCAST [2] extended OMA DRM v2.0 [4] for broadcast service environment. Smartcard profile in OMA BCAST [2] extends multimedia broadcast multicast service (MBMS) [5, 6] and broadcast and multicast services (BCMCS) [7, 8] with generic bootstrapping architecture (GBA) [9] for service and content protection in broadcast environment.

The current mobile broadcast DRM systems do not provide efficient solution for rights portability with the user identity card (UIC). Rights portability means consuming broadcast service using the UIC (i.e., independent of specific terminals). This prevents users from consuming broadcast service and contents independent of a specific terminal (e.g., the one used for registration or purchase). For example, the DRM profile [2] and 18Crypt [1] are mainly based on authentication between the terminal and the service provider. Even though the smartcard profile [2] uses universal subscriber identity module (USIM) [10] or removable user identity module (R-UIM) [11], but it does not provide efficient mechanism for rights portability in mobile broadcast services.

The rights portability with the UIC can be implemented by rendering broadcast services with multiple terminals using the user identity card storing rights. Whenever a new terminal is used for consumption of broadcast services, security associations need to be established among the service provider, the terminal, and the UIC. The UIC usually interacts with a terminal for sensitive data exchanged between the two. Therefore, the need to establish a secure channel between the UIC and the terminal has been identified in order to protect the communication between them. We list the following requirements for rights portability with the UIC:

(1) mutual authentication between the terminal and the UIC;

(2) mutual authentication between the terminal and the service provider;

(3) mutual authentication between the UIC and the service provider;

(4) secure channel establishment between the terminal and the UIC.

Previous authentication protocols [12–14] and DRM systems using the user identity [15, 16] do not satisfy above security requirements for mobile broadcast systems. The smartcard profile [2] provides rights portability using (U)SIM or (R-)UIM, however, it suffers from inefficiency due to execution of different authentication protocols and lots of

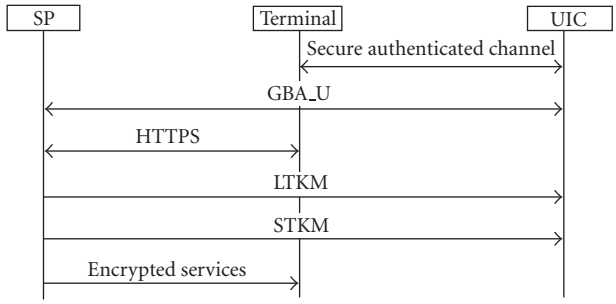

Figure 1: Function flow of the smartcard profile.

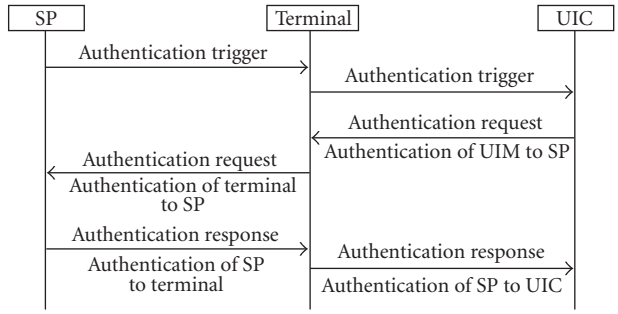

Figure 2: Overview of the proposed scheme.

message exchanges from GBA_U [9], HTTPS [17], and secure channel establishment [18] as shown in Section 2.

In this paper, we propose the new authentication scheme which satisfies the above requirement. We also present the mobile broadcast DRM based on the proposed authentication scheme for rights portability. The proposed authentication scheme provides efficient way for mutual authentications among the SP, the terminal, and the UIC.

This paper is organized as follows. We provide brief look at the prior mobile broadcast DRM system in Section 2. The overview of the proposed scheme is shown in Section 3. We propose the new authentication scheme satisfying the above requirements in Section 4. We utilize the proposed authentication protocol for mobile broadcast DRM based on the UIC in Section 5. We provide security analysis of the proposed scheme and comparison with the previous work in Section 6. Concluding remarks are shown in Section 7.

2. PREVIOUS WORK

The smartcard profile [2] provides service and content protection method in the mobile broadcast system. It uses the (U)SIM [10] or (R-)UIM [11] to receive and store the rights for rendering protected service for rights portability, that is, consuming the protected service using various terminals with the UIC. Figure 1 shows the high level function flow of the smartcard profile [3].

As illustrated in Figure 1, the smartcard profile [3] uses GBA_U [9] for mutual authentication between the terminal and the UIC. HTTPS [17] is run between the service provider (SP) and the terminal for mutual authentication. The secure authenticated channel (SAC) is established between the terminal and the smartcard by [18].

The service encryption key (SEK) or the program encryption key (PEK) is packaged in a special long-term key message (LTKM) format. Pay-per-view customers are provided with a PEK that is only valid for a single program while subscribers would be provided with a SEK, valid for reception of the service for some longer period.

The traffic encryption key (TEK) is applied to the actual content following different mechanisms depending on the actual encryption method used. The TEKs are themselves sent encrypted by a SEK or a PEK. The message carrying encrypted TEK is called the short-term key message (STKM).

The smartcard profile [2] provides rights portability using (U)SIM or (R-)UIM, however, it suffers from inefficiency due to execution of different authentication protocols and lots of message exchanges from GBA_U [9], HTTPS [17], and secure channel establishment [18]. The proposed scheme provides enhanced efficiency as shown in Sections 3 and 4.

3. OVERVIEW OF THE PROPOSED SCHEME

In this section, we show overview of the proposed authentication scheme. The proposed protocol plays a critical role for a user to consume purchased broadcast contents independent of specific terminals (e.g., the one used for purchase) for rights portability. Unlike the previous work as described in Section 2, the proposed scheme provides mutual authentication among the SP, the terminal, and the UIC in one combined protocol. We denote a user identity card as the UIC and also denote the service provider as the SP in the rest of this paper.

The overview of the proposed scheme is shown in Figure 1 and described in the following.

(1) The SP provides authentication trigger message to the terminal. For example, the authentication trigger message can be embedded in the service guide [2].
(2) On receipt of the message in step (1), the terminal forwards the trigger message to the UIC.
(3) On receipt of the message in step (2), the UIC generates digital signature using a random number from the SP. The UIC delivers the digital signature and its own identity to the terminal. This message represents authentication of the UIC to the SP.
(4) On receipt of the message in step (3), the terminal also generates digital signature and delivers the digital signature and its identity to the SP. This message represents authentication of the terminal to the SP.
(5) On receipt of the message in step (4), the SP receives digital signatures from the terminal and the UIC and verifies them. If the verification is successful, the SP generates its digital signature and authentication result of the terminal and the UIC, respectively. The SP sends the message to the terminal. This message represents authentication of the SP to the terminal.
(6) On receipt of the message in step (5), the terminal receives the authentication result of the UIC and verifies

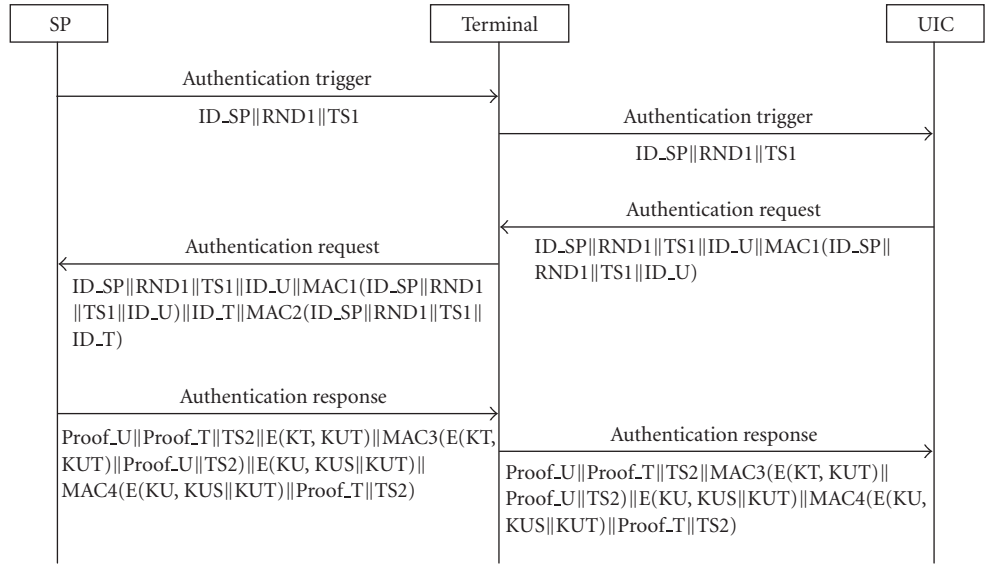

Figure 3: Proposed authentication protocol based on symmetric key cryptosystem.

digital signature from the SP. The terminal also forwards the message to the UIC. This message represents authentication of the SP to the UIC.

(7) On receipt of the message in step (6), the UIC receives the message from the terminal and verifies the authentication result of the terminal. If the verification is successful, then the UIC allows communication with the terminal.

4. PROPOSED AUTHENTICATION PROTOCOLS

This section shows the proposed authentication protocols for mutual authentications among the SP, the terminal, and the UIC and secure channel establishment between the terminal and the UIC. We show the proposed protocol based on both symmetric key cryptosystem in Section 4.1 and public key cryptosystem in Section 4.2.

4.1. Authentication protocol based on symmetric key cryptosystem

The following protocol in Figure 3 shows the proposed authentication with symmetric key-based system. In the protocol, we assume that the UIC shares a symmetric key, KU, with the SP for encryption and generation of message authentication code. We also assume that the terminal and the SP shares a symmetric key, KT, for encryption and generation of message authentication code. We described the following protocol independent of specific encryption and message authentication algorithms.

In the following, we provide description of the proposed authentication protocol which works based on symmetric key cryptosystem. We assume that there is a shared key, KU, between the SP and the UIC and also assume that there is a shared key, KT, between the SP and the terminal before the protocol starts.

(1) The SP sends authentication trigger message which consists of identity of SP ID_SP, random number RND1, and time stamp, TS1.

(2) On receipt of the message in step (1), the terminal forward authentication trigger message to the UIC.

(3) On receipt of the message in step (2), the UIC adds its identity ID_U and generates message authentication code MAC1 on this message using the symmetric key shared with the SP before the protocol starts. The UIC forwards this message to the terminal

(4) On receipt of the message in step (3), the terminal adds its own identity ID_T and generates message authentication code MAC2 on ID_SP, RND1, TS1 and ID_T. Terminal directly forwards authentication request message to the SP.

(5) On receipt of the message in step (4), the SP generates Proof_U and Proof_T, containing authentication result of the UIC and terminal, respectively, based on the verification result of MAC1 and MAC2. The SP generates the time-stamp, TS2, and generates encryption of KUT, a session key between the UIC and terminal, and KUS, a new shared key between the smartcard and SP, using KU. The SP also generates the encryption of KUT using KT. The SP generates the message authentication code, MAC3, on E(K_T, KUT), Proof_U, and TS2 for the terminal to verify it. The SP also generates the message authentication code, MAC4, on E(KU, KUS || KUT), Proof_T, and TS2 for the UIC to verify it. The SP sends this message to the terminal.

(6) On receipt of the message in step (5), the terminal verifies MAC3 and can be assured that whether integrity of the message is correct or not. After verification of Proof_U, the terminal can find out that whether the UIC can be trusted or not. The terminal decrypts E(KT, KUT) using KT and verifies MAC2. Finally, the terminal forwards the message to the UIC.

(7) On receipt of the message in step (6), the UIC verifies MAC4 and can be assured that whether integrity of the message is correct or not. After verification of Proof_T, the UIC can find out that whether the terminal can be trusted or not. The UIC acquires KUS and KUT by decryption of E(KU, KUS || KUT) using KU.

After the successful run of the above protocol, the UIC and the terminal establish a common secret key the KUT. The UIC also acquires a new session key between the SP and itself. For efficiency, the terminal may not forward some elements related to itself to the UIC in the last message.

4.2. Authentication protocol based on public key cryptosystem

The following protocol in Figure 4 shows the proposed authentication protocol based on the public key cryptosystem. Unlike the previous protocol, we assume that the terminal and the SP has public key and private key for encryption and digital signature operations such as RSA [19]. We also assume that the UIC shares a symmetric key with the SP for encryption and digital signature operations. We described the following protocol independent of specific public key encryption and digital signatures mechanisms.

In the following, we provide description of the proposed authentication protocol which works based on public key cryptosystem. We assume that there is a public and private key pair for the terminal and the SP, respectively, and also assume that there is a shared key KU between the SP and the UIC before the protocol starts.

(1) The SP sends authentication trigger message which consists of identity of SP ID_SP, random number RND1, and time stamp, TS1.
(2) On receipt of the message in step (1), the terminal forward authentication trigger message to the UIC.
(3) On receipt of the message in step (2), the UIC adds its identity ID_U and generates message authentication code MAC1 on this message using the symmetric key shared with the SP before the protocol starts. The UIC forwards this message to the terminal.
(4) On receipt of the message in step (3), the terminal adds its own identity ID_T and generates the digital signature on ID_SP, RND1, TS1, and ID_T using its private key. The terminal directly forwards authentication request message to the SP.
(5) On receipt of the message in step (4), the SP generates Proof_U and Proof_T, containing authentication result of the UIC and the terminal, respectively, based on the verification result of MAC1 and Sign_T. The SP generates the time-stamp, TS2, and generates encryption of KUT, a session key between the UIC and terminal, and KUS, a new shared key between the UIC and SP, using KU. The SP also generates the encryption of KUT using PK_T which is the public key of the terminal. The SP generates the digital signature, Sign_SP, on encryption of KUT E(PK_T, KUT), Proof_U, and TS2 for the terminal to verify it. The SP also generates the message authentication code, MAC2, on E(KU, KUS || KUT), Proof_T and time-stamp from the SP, TS2, for the UIC to verify it. The SP sends this message to the terminal.
(6) On receipt of the message in step (5), the terminal verifies Sign_SP and can be assured that whether integrity of the message is correct or not. After verification of Proof_U, the terminal can find out that whether the Smartcard can be trusted or not. The terminal decrypts E(PK_T, KUT) using its private key. After that, the terminal forwards the message to the UIC.
(7) On receipt of the message in step (6), the UIC verifies MAC2 and can be assured that whether integrity of the message is correct or not. After verification of Proof_T, the UIC can find out that whether the terminal can be trusted or not. The UIC acquires KUS and KUT by decryption of E(KU, KUS || KUT) using KU.

After the successful run of the above protocol, the UIC and the terminal establish a common secret key the KUT. The UIC also acquires a new session key between the SP and itself. For efficiency, the terminal may not forward some elements related to itself to the UIC in the last message.

5. MOBILE BROADCAST DRM WITH THE PROPOSED AUTHENTICATION PROTOCOL

In this section, we show how the proposed authentication protocol can be used for rights portability in the mobile broadcast system. The mobile broadcast DRM system with the proposed authentication scheme shown in Section 4 consists of two phases. The terminal executes the proposed authentication protocol during registration procedure in the first phase. When the UIC is in contact with a new terminal, it runs the proposed authentication protocol for mutual authentication with the terminal and SP in the second phase.

5.1. Mobile broadcast system with the proposed authentication scheme

This section shows the overall flow for mobile broadcast DRM system with the proposed authentication protocol. This following procedure is run when a user subscribes a new service to acquire the SEK. The procedure is shown in Figure 5 and described in the following.

(1) The UIC runs the proposed authentication protocol with the SP. The proposed protocol can be run in part of the registration procedure.
(2) The terminal transfers service request containing identity of the UIC, ID_U, Service ID, and a random number, RND1, to the SP for acquisition of SEK.
(3) The terminal receives service response message from the SP and forwards it to the UIC. The UIC stores the RO in secure memory area. The RO contains SEK or PEK.
(4) The UIC acquires the rights object from the SP, extracts SEK from the RO, and stores SEK in secure memory area in the UIC.
(5) The SP broadcasts traffic key message in encrypted form. The UIC receives the message and extracts the

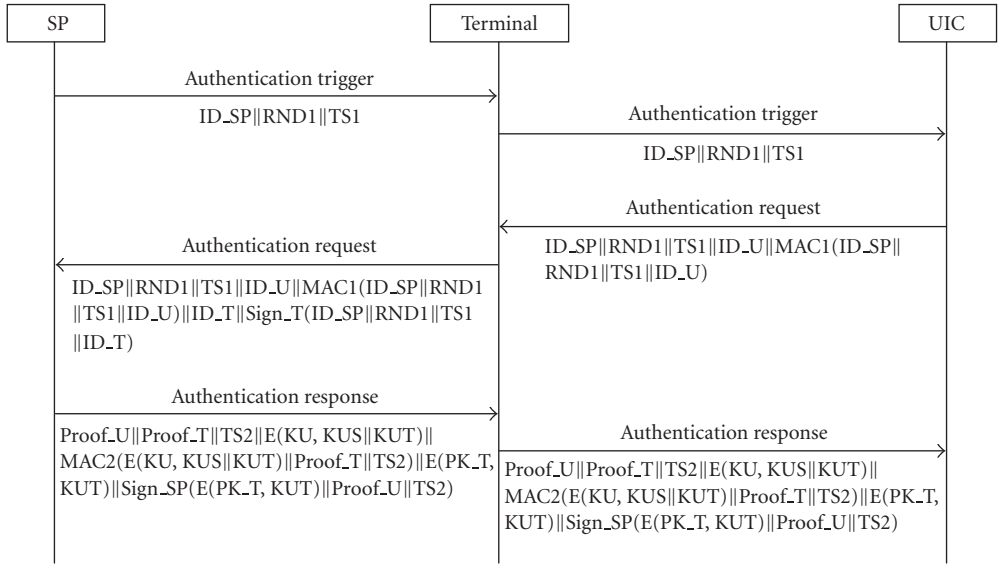

Figure 4: Proposed authentication protocol based on public key cryptosystem.

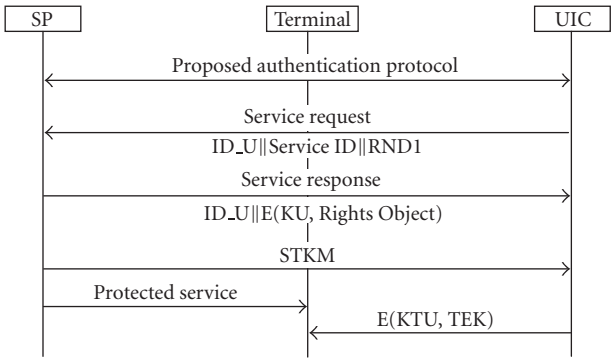

Figure 5: Mobile broadcast system with the proposed authentication scheme.

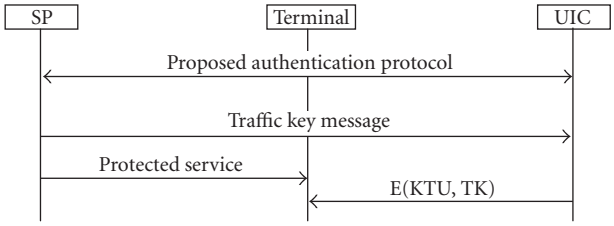

Figure 6: The terminal change and the proposed authentication scheme.

TK. The UIC forwards the TK in secure channel established by KUT.

(6) The terminal can decrypt the encrypted TK by KUT and use TK for decryption of protected services and contents.

The UIC stores KU and KUT in secure memory area for further use in the next step shown in Section 5.2.

5.2. Terminal change and the proposed authentication scheme

When the UIC is in contact with a new terminal, the UIC and the terminal executes the proposed authentication protocol with the SP to establish security association.

(1) The terminal and the UIC runs the proposed authentication protocol with the SP. A new secure channel is established between the terminal and the UIC.

(2) The SP broadcasts a traffic key message to the terminal. The terminal forwards it to the UIC.

(3) The UIC extracts TK from the message and forwards it to the terminal in secure channel.

(4) The terminal can acquire TK by KTU. The terminal can decrypt the protected service using TK.

After the successful authentication of the terminal and the UIC by the SP, the SP provides KTU to the terminal and the UIC for establishment of the secure channel. The terminal and the UIC also authenticate each other through the execution of the above protocol.

6. ANALYSIS

6.1. Security

The proposed mobile broadcast DRM system, shown in Section 5, provides terminal independent use of broadcast services with the UIC based on the proposed authentication scheme. Unlike the previous work, mutual authentications among the SP, the terminal and the UIC are satisfied through the terminal. In the following, we show analysis of important properties of the proposed authentication scheme. These requirements are shown in Section 1.

Table 1: Comparison with previous works.

	GBA_U	HTTPS	SAC	Proposed scheme
Mutual authentication between the terminal and the UIC	No	No	Yes	Yes
Mutual authentication between the UIC the SP	Yes	No	No	Yes
Mutual authentication between the terminal and the SP	No	Yes	No	Yes
Secure channel between the terminal and the UIC	No	No	Yes	Yes
Number of messages	4	≒ 10	9	6

Mutual authentication between the UIC and the terminal

Proof_U and Proof_T generated by the SP contains the authentication result of the UIC and the terminal. The terminal can authenticate the UIC by verifying the Proof_U and the SP can authenticate the terminal by verifying the Proof_T in the proposed authentication protocol.

Mutual authentication between the UIC and the SP

The SP can authenticate the UIC by verifying MAC1 in the authentication protocol. MAC1 contains a random number from the SP. The UIC can also authenticate the SP by verifying MAC4 or Sign_SP from the SP in the authentication protocol.

Mutual authentication between the terminal and the SP

The SP can authenticate the terminal by verifying MAC2 or Sign_T in the authentication protocol. MAC2 contains a random number from the SP. The terminal can also authenticate the SP by verifying MAC3 or Sign_SP from the SP in the authentication protocol.

Secure channel between the terminal and the UIC

This property can be achieved by the secure channel represented by the key KTU shared between the terminal and the UIC.

6.2. Comparison

Table 1 shows comparison between the proposed scheme and the previous works for mutual authentication among the SP, the terminal, and the UIC. The previous work, as shown in Section 2, suffers from the use of multiple authentication and key establishment mechanisms such as GBA_U, HTTPS, and SAC. The proposed protocol achieves all properties of previous protocols in one protocol with enhanced efficiency.

7. CONCLUDING REMARKS

In this paper, we proposed the new authentication scheme providing mutual authentications among the SP, the terminal and the UIC. The secure channel between the terminal, and the UIC is also established as part of the proposed scheme. The previous work, as shown in Section 2, suffers from the use of multiple authentication and key establishment mechanisms such as GBA_U, HTTPS, and SAC, but the proposed protocol achieves all properties of previous protocols in one protocol with enhanced efficiency. We utilized the proposed protocol for rights portability based on the UIC in the mobile broadcast system. The proposed mobile broadcast system allows a user to consume broadcast services and contents independent of specific terminals (e.g., the one used for registration or purchase) with enhanced efficiency.

REFERENCES

[1] IP Datacast over DVB-H: Service Purchase and Protection (SPP), DVB, 2006.
[2] OMA BCAST v1.0 enabler, Open Mobile Alliance, http://www.openmobilealliance.org/.
[3] Service Content Protection Specification, Open Mobile Alliance, http://www.openmobilealliance.org/.
[4] OMA-DRM-V2_0 enabler, "Open Mobile Alliance™," http://www.openmobilealliance.org/.
[5] 3GPP TS 26.346, "Multimedia broadcast/multicast service (MBMS); protocols and codecs," 3rd Generation Partnership Project, Technical Specification 3GPP TS 26.346, http://www.3gpp.org/.
[6] 3GPP TS 33.246, "Security of multimedia broadcast/multicast service," 3rd Generation Partnership Project, Technical Specification 3GPP TS 33.246, http://www.3gpp.org/.
[7] 3GPP2 X.S0022, "Broadcast and multicast service in cdma2000 wireless IP network," 3rd Generation Partnership Project 2, Technical Specification 3GPP2 X.S0022, http://www.3gpp2.org/.
[8] 3GPP2 S.S0083, "BCMSC security framework," 3rd Generation Partnership Project 2, Technical Specification 3GPP2 S.S0083, http://www.3gpp2.org/.
[9] 3GPP TS 33.220, "Generic authentication architecture, generic bootstrapping architecture," 3rd Generation Partnership Project, Technical Specification 3GPP TS 33.220, http://www.3gpp.org/.
[10] 3GPP TS 31.102, "Characteristics of the universal subscriber identity module (USIM) application," 3rd Generation Partnership Project, Technical Specification 3GPP TS 31.102, http:// www.3gpp.org/.
[11] 3GPP2 C.S0023, "Removable user identity module for spread spectrum systems," 3rd Generation Partnership Project 2, Technical Specification 3GPP2 C.S0023, http://www.3gpp2.org/.
[12] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.
[13] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.
[14] S. P. Miller, B. C. Neuman, J. I. Schiller, and J. H. Saltzer, "Section E.2.1: Kerberos authentication and authorization system,"

Tech. Rep., M.I.T. Project Athena, Cambridge, Mass, USA, December 1987.

[15] C. Conrado, F. Kamperman, G. J. Schrijen, and W. Jonker, "Privacy in an identity-based DRM system," in *Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA '03)*, pp. 389–395, Prague, Czech Republic, September 2003.

[16] T. Kalker, M. Spasojevic, A. Said, A. Petruszka, P. Shah, and P. Mclean, "A case for person-centric digital rights management," in *Proceedings of the IEEE Consumer Communications & Networking Conference, (Workshop on Digital Rights Management Impact on Consumer Communications) (CCNC '05)*, Las Vegas, Nev, USA, January 2005.

[17] E. Rescorla, "HTTP over TLS," RFC 2818, http://www.ietf.org/rfc/rfc2818.txt.

[18] 3GPP TS 33.110, "Key establishment between a UICC and a terminal," 3rd Generation Partnership Project, Technical Specification 3GPP TS 33.110, http://www.3gpp.org/.

[19] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.