

Internet Draft
Document: draft-urien-eap-smartcard-type-00.txt

P.Urien
ENST
W.Habraken
RAAK Technologies
D. Flattin
Oberthur Card Systems
H. Ganem
Axalto
March 2005

Expires:

EAP Smart Card Protocol (EAP-SC)

Status of this Memo

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, or will be disclosed, and any of which I become aware will be disclosed, in accordance with RFC 3668.

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet Drafts.

Internet-Drafts are draft documents valid for a maximum of six Months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at
<http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>

Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

1 Abstract

Smart Cards are hardware security devices that are widely used in data and voice networks to authenticate users and devices, and to enforce security policies on the client platform.

The EAP Smart Card Protocol (EAP-SC) defines an EAP Method and Multiplexing model for the support of Smart Card based authentication methods. EAP-SC provides a uniform framework for interfacing with Smart Cards within the EAP [RFC3748] context. EAP-SC provides for encapsulation of other EAP methods (such as [EAP-TLS], [EAP-SIM] and [EAP-AKA]).

EAP-SC enhances the security of authentication methods by enabling the use of Smart Cards for the secure provisioning and storage of keys and credentials, and the secure execution of security sensitive functions. In addition, EAP-SC provides security requirements for the support of Smart Card based Authentication Methods that ensure a uniform level of security complementary to the underlying authentication method.

Table of Contents

1	Abstract.....	2
2	Terminology.....	3
3	Architecture.....	3
	3.1 EAP Methods and Smart Cards.....	3
	3.2 The EAP-SC Multiplexing Model.....	4
	3.3 Smart Card Support.....	5
4	Protocol Overview.....	5
	4.1 EAP-SC Packets.....	5
	4.2 EAP Packet Handling at the Peer Side.....	7
	4.2.1 Incoming EAP Packet Handling at the Peer Side.....	7
	4.2.2 Outgoing EAP Packet Handling at the Peer Side.....	7
	4.3 EAP Packet Handling at the Authentication Server Side.....	7
	4.3.1 Incoming EAP Packet Handling at the Authentication Server Side.....	7
	4.3.2 Outgoing EAP Packet Handling at the Authentication Server Side.....	7
5	IANA considerations.....	8
6	Security Considerations.....	8
	6.1 Threat Model.....	8
	6.2 Smart Card Security Capabilities and Requirements.....	8
	6.2.1 Smart Card Technology.....	9
	6.2.2 Tamper Resistant Storage and Execution.....	9
	6.2.3 Multi Factor Authentication.....	9
	6.2.4 Random Number Generation.....	9
	6.2.5 Cryptographic Capabilities.....	9
	6.2.6 Secure Provisioning.....	10
	6.2.7 Certification.....	10
	6.3 Smart Cards and EAP Security Claims.....	10

6.3.1	Mutual Authentication.....	10
6.3.2	Confidentiality.....	10
6.3.3	Key Derivation.....	11
6.3.4	Man-in-the-Middle Attacks.....	11
6.3.5	Dictionary Attacks.....	11
6.3.6	Cryptographic Binding.....	11
6.3.7	Channel Binding.....	11
6.3.8	Protection Against Rogue Networks.....	11
6.3.9	Authentication Method Security.....	11
7	Security Claims.....	12
8	References.....	12
9	Author's Addresses.....	13
10	Intellectual Property Statement.....	14
11	Disclaimer of Validity.....	14
12	Copyright Statement.....	14
13	Acknowledgment.....	14

2 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119.

EAP Smart Card

A Smart Card that supports an EAP authentication method on the smart card, such as a smart card conforming to [SC-EAP] or [UICC-EAP].

Smart Card EAP packet [SC EAP packet]

An RFC3748 compliant EAP method packet to be managed by an EAP Smart Card.

EAP-SC Authentication Method

An Authentication Method implemented on a Smart Card within the framework of EAP-SC, typically an EAP Authentication Method such as EAP-TLS.

3 Architecture

3.1 EAP Methods and Smart Cards

According to [RFC3748], EAP methods implement the authentication algorithms, handle fragmentation and receive and transmit EAP messages via the EAP Peer and Authentication Server layers.

When an EAP Method uses a Smart Card, a Smart Card Handler is required to manage communication between the EAP Peer Layer and the Smart Card, and to handle any required user interface and card management functions.

Within the EAP multiplexing model, the overall EAP Method functionality is split between the Smart Card Handler and the Smart Card functions or applications.

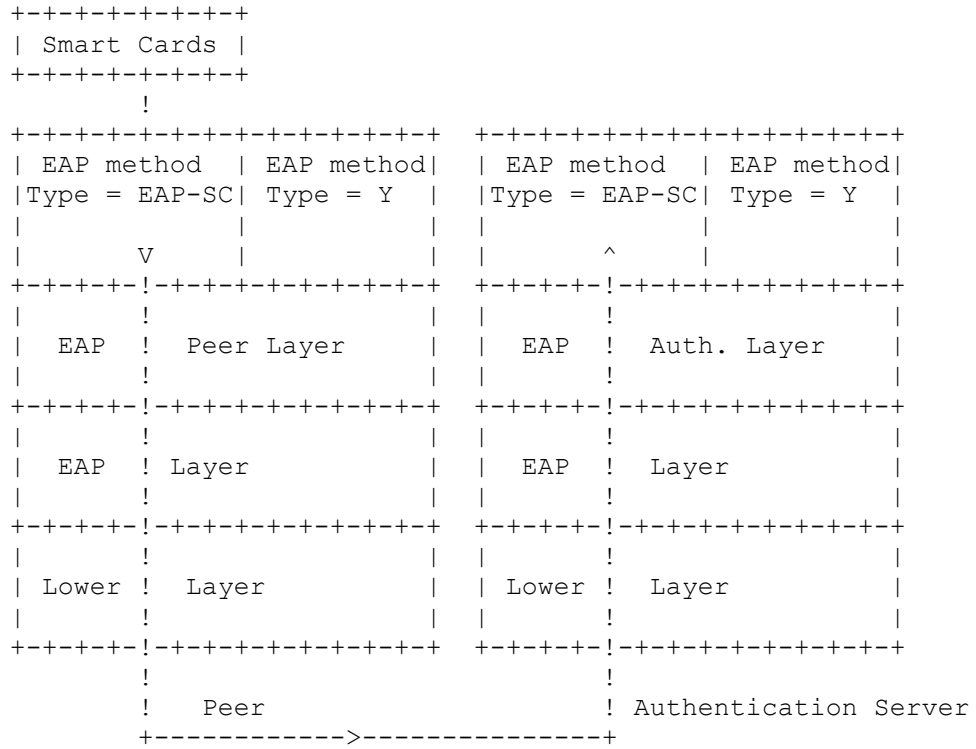


Figure 1: The Smart Card in the EAP Multiplexing Model

3.2 The EAP-SC Multiplexing Model

The EAP-SC Multiplexing model addresses the fact that Smart Cards can be removed and multiple Smart Cards can be used with a peer. In addition, many types of Smart Card types may be supported, and each Smart Card type may support one or multiple authentication methods and credentials. For this reason, EAP-SC must query the Smart Card and determine the type of card and application before initiating the EAP transaction.

The EAP-SC model consists of three layers.

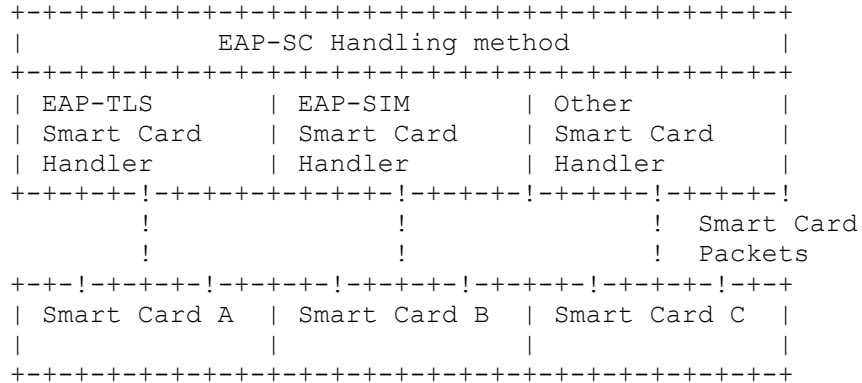


Figure 2: EAP-SC Multiplexing Model

The EAP-SC handling layer receives and sends EAP packets, selects a Smart Card handler, and passes packets to the Smart Card handler.

The EAP Smart Card Handler layer handles the interface to the smart card, as well as any EAP Method specific functions that are not handled in the smart card.

The Smart Card executes security sensitive Authentication Method functions in conjunction with the EAP Smart Card Handler.

3.3 Smart Card Support

The EAP-SC method MUST be compatible with [SC-EAP] and [UICC-EAP] type Smart Cards that implement [EAP-TLS]. The EAP-SC method MAY support smart cards supporting [EAP-SIM], [WLAN-SIM], [EAP-AKA], [EAP-PEAP], [EAP-TTLS].
 EAP-SC MUST NOT support any Smart Card based EAP Method that does not meet the security requirements in section 6.

4 Protocol Overview

4.1 EAP-SC Packets

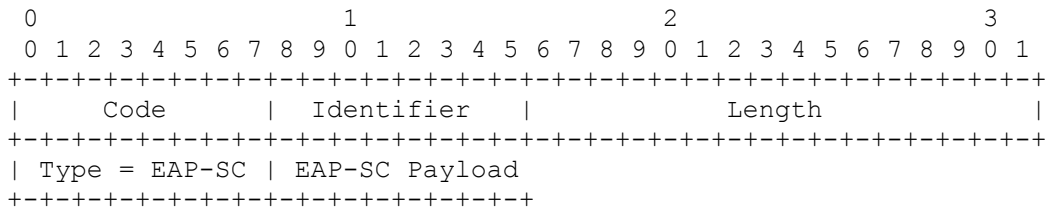


Figure 3: Format of EAP-SC packet

A packet is sent to the EAP-SC Handler when its Type [RFC3748] is equal to the EAP-SC value.

The EAP-SC payload is the same format as the Expanded Type described in section 5.7 of [RFC 3748].

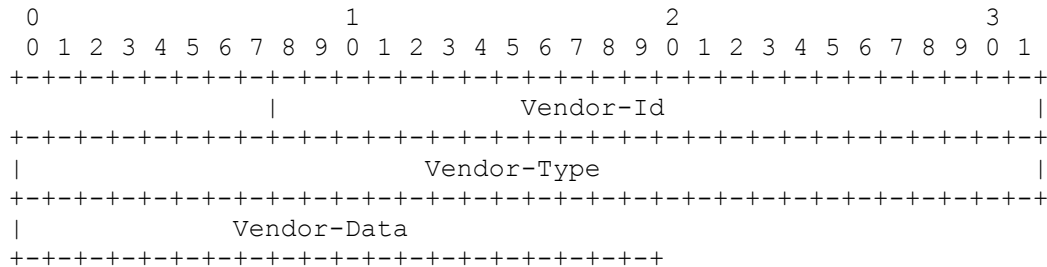


Figure 4: EAP-SC Payload packet format

- Vendor-Id, three bytes set to zero, Reserved for Future Use
- Vendor-Type, four bytes. The first three significant bytes are null, the least significant byte (Vendor-Type[7,0]) represents the EAP-Type to be processed by the Smart Card.
- Vendor-Data, represents the EAP method packet (without the Code, Identifier and Length fields) to be processed by the EAP Smart Card [SC-EAP] or [UICC-EAP].

The complete EAP-SC packet structure with its transported EAP method packet or Smart Card EAP packet is as follow.

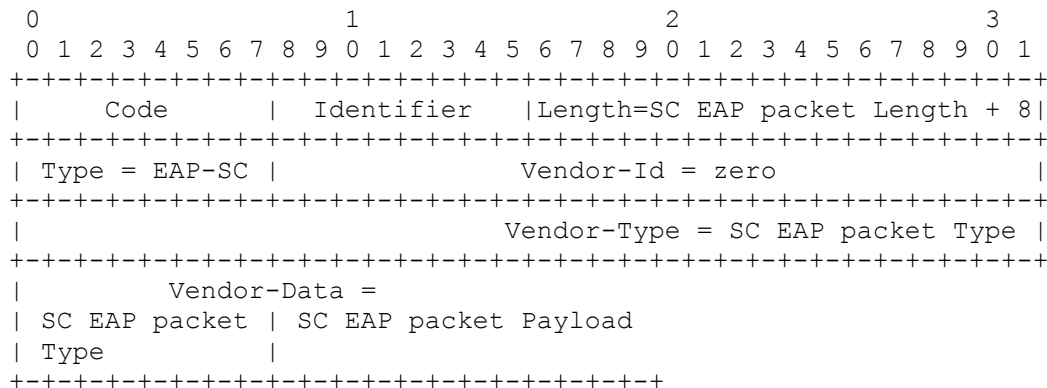


Figure 5: EAP-SC EAP Packet encoding

- The Code field MUST be identical to the transported Smart Card EAP packet Code.

- The Identifier MUST be identical to the transported Smart Card EAP packed Identifier.
- The Length field MUST be equal to the transported Smart Card EAP packet Length plus 8.
- The Type field MUST be set to EAP-SC Type.
- The Vendor-Id field MUST be set to zero.
- The Vendor-Type field MUST be set to zero for the 3 most significant bytes and set to the transported Smart Card EAP packet Type for the last significant byte.
- The Vendor-Data field MUST contain the transported Smart Card EAP packed Type and Payload.

4.2 EAP Packet Handling at the Peer Side

4.2.1 Incoming EAP Packet Handling at the Peer Side

The EAP-SC layer rebuilds the transported EAP method packets to be processed by the Smart Card.

The EAP-SC layer modifies the incoming EAP-SC packets by removing the EAP-SC Type, the Vendor-Id and the Vendor-Type fields and by subtracting the Length field by 8. Then the EAP message is forwarded to the appropriate Smart Card Handler, such as [WLAN-SC].

4.2.2 Outgoing EAP Packet Handling at the Peer Side

The EAP-SC layer builds the EAP-SC EAP packet from the Smart Card EAP packet to transport.

The EAP-SC layer modifies the Smart Card EAP packets by inserting the EAP-SC Type, the Vendor-Id, the Vendor-Type fields and by setting Vendor-Type field with the transported Smart Card EAP Type and adding the Length value with 8. Then, packets are sent to the Authentication Server.

4.3 EAP Packet Handling at the Authentication Server Side

4.3.1 Incoming EAP Packet Handling at the Authentication Server Side

The EAP-SC layer modifies the Incoming EAP-SC packets by removing the EAP-SC Type, the Vendor-Id and the Vendor-Type fields and by subtracting the Length field by 8. Then, the EAP packets MUST be processed by the Authentication Server.

4.3.2 Outgoing EAP Packet Handling at the Authentication Server Side

The EAP-SC layer modifies the Outgoing EAP-SC packets by inserting the EAP-SC Type, the Vendor-Id, the Vendor-Type fields and by setting Vendor-Type field with the transported EAP Type and adding the Length value with 8. Then the authentication server MUST send the packets to the Peer.

5 IANA considerations

EAP-SC type is set to xx

6 Security Considerations

6.1 Threat Model

An attacker may attack a typical EAP transaction by compromising the peer. For example, an attacker may gain access to genuine keys and credentials and share these with an unauthorized user. Or an attacker may gain access and modify cryptographic processes as they are executed on the peer platform.

Security policies must be established to secure against such peer attacks. The EAP-SC type makes it possible to enforce security policies by using smartcards.

This includes scenarios which require strong authentication of the end user, where the end user platform is vulnerable to direct attack, where the end user may be considered an enabling agent in the attack, or where the enforcement of end user policies is subject to legal requirements. Examples of such scenarios are:

- A service provider wanting to grant subscribers access to network based value added services
- A hospital subject to medical privacy regulations that needs to assure that only authorized personnel can access patient information.
- A government organization which needs to secure classified information

6.2 Smart Card Security Capabilities and Requirements

Smart cards are a highly effective means of enforcing security policies. Smart cards are typically carried by one party (the end user, such as an employee or customer) but are controlled by another party (the issuer, such as an enterprise or service provider). Applications running on the Smart Card are controlled by the issuer, and serve to protect the interests of the issuer.

The following sub sections describe Smart Card security capabilities and requirements for EAP-SC Authentication Methods relating to those capabilities:

6.2.1 Smart Card Technology

The Smart Card consists of a microprocessor and non-volatile memory chipset enclosed in a physically tamper resistant module. This module is then embedded in a plastic card, or the module may be integrated into an alternative form factor, such as a USB device.

6.2.2 Tamper Resistant Storage and Execution

Smart cards provide protective measures against physical and logical attacks against the processor and non-volatile memory. This enables the secure storage of end user cryptographic keys and user credentials, and secures execution of security sensitive operations such as encryption and digital signatures.

The EAP-SC Authentication Method MUST store all secret cryptographic keys on the smart card in non-volatile memory. The EAP-SC Authentication Method MUST execute in the smart card all cryptographic functions that use stored secret cryptographic keys. The EAP-SC Authentication Method MUST NOT export any secret cryptographic keys from the smart card.

6.2.3 Multi Factor Authentication

Smart cards generally require a Smart Card handler to authenticate to the Smart Card in order to access data or application functionality. This makes it possible to enforce multi factor user authentication by combining something the user has (the smart card) with something the user knows (such as PIN) or is (Biometric authentication).

The EAP Authentication Method MUST enforce the use of the user PIN or Biometric before user credentials may be accessed or used.

6.2.4 Random Number Generation

Smart Cards generally contain a hardware based true random number generator independent of external or internal clocks and immune to outside interferences. The quality of the hardware generator is further enhanced by logical processing to ensure excellent statistical properties; and these properties are checked regularly on-board.

The EAP Authentication Method MUST use the Smart Card Random Number Generator anywhere Random Numbers are required.

6.2.5 Cryptographic Capabilities

Smart cards provide certified, built-in implementation and optimised execution of common cryptographic algorithms such as AES, DES, RSA, and ECC...

The EAP Authentication Method MUST use the built-in Smart Card cryptographic capabilities for the execution of any cryptographic functionality.

6.2.6 Secure Provisioning

Smart cards provide a secure method of provisioning credentials, applications and trusted network information from the issuer or service provider to the end user, and managing this information after the card has been issued. Smart cards support automated personalization (including card initialization, loading of card data and printing) enabling issuance in very large numbers.

The EAP-SC Authentication method MUST implement support for pre-issuance personalization, as for example by supporting [GLOBAL PLATFORM] or similar functionality. The EAP-SC Authentication method SHOULD implement support for post-issuance card and application management.

6.2.7 Certification

The processes for designing and manufacturing smart cards are subject to rigorous security controls. This makes possible the certification of Smart Card functionality and applications by standardization organizations.

The EAP-SC Authentication method MUST be implemented on a Smart Card platform that has been evaluated for security by a standards organization program such as [FIPS] or [COMMON CRITERIA].

6.3 Smart Cards and EAP Security Claims

EAP-SC enhances the security of Authentication Methods by enabling the enforcement of security policies on the End User platform. The overall security of EAP-SC is dependent on the security of the Authentication Method implemented on the Smart Card.

The following section discusses certain EAP Security Claims and how they are enhanced by Smart Card security features.

6.3.1 Mutual Authentication

Mutual authentication processes are generally based upon the use of random numbers. Smart Cards enhance the security of these processes by providing true random number generation.

6.3.2 Confidentiality

Smart Cards improve the robustness of EAP messages encryption, by providing tamper resistant storage for the encryption keys and secure execution of the encryption algorithms.

6.3.3 Key Derivation

Smart Cards improve the confidentiality of the key derivation process by providing tamper resistant storage for the master keys and secure execution of the key derivation algorithms.

6.3.4 Man-in-the-Middle Attacks

Smart Cards improve security against Trojan Horse attacks by providing a logically tamper resistant environment for the full implementation of EAP methods and secure execution of the encryption algorithms.

6.3.5 Dictionary Attacks

Smart Cards access is commonly protected via pin codes with a limited number of retries; permanent blocking of the device is enforced when the number of retries is exceeded. This mechanism provides enhanced protection against dictionary attacks aiming at discovering passwords.

6.3.6 Cryptographic Binding

Smart Cards provides tamper resistant storage for cryptographic keys and secure execution of the tunnel creation algorithms thus enhancing the cryptographic binding process.

6.3.7 Channel Binding

Smart Cards can be used as a secure out of band distribution method for channel parameters and therefore enhance the channel binding process.

6.3.8 Protection Against Rogue Networks

Smart Cards facilitate the provisioning and secure storage of information about trusted parties, such as the root certificates of trusted networks. This protects the end user against rogue networks and enables the enforcement of network roaming policies.

6.3.9 Authentication Method Security

The overall security of EAP-SC is dependent on the encapsulated EAP-SC Authentication Method. Weaknesses in the underlying method, such as weaknesses in integrity protection, replay protection or key strength, are detrimental to the overall security.

7 Security Claims

Integrity Protection: no
Replay Protection: no
Confidentiality: yes (section 6.3.2)
Key Derivation: yes (section 6.3.3)
Key Strength: no
Dictionary Attacks: yes (section 6.3.4)
Fast Reconnect: no
Cryptographic Binding: yes (section 6.3.6)
Session Independence: no
Fragmentation: no
Channel Binding: yes (section 6.3.7)

8 References

- [RFC 3748], Extensible Authentication Protocol (EAP), B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, June 2004.
- [SC-EAP], draft-urien-eap-smartcard-06.txt, P.Urien, A.J. Farrugia, M.Groot, G.Pujolle, J. Abellan, September 2004
- [UICC-EAP] European Telecommunications Standards Institute, ETSI TS 102.310 Extensible Authentication Protocol support in the UICC
- [WLAN-SIM] WLAN-SIM specification V1.0, WLAN Smart Card Consortium, October 20, 2003
- [WLAN-SC] Wlan Smart Card Handler Specification, WLAN Smart Card Consortium, - in progress -
- [EAP-SIM] Extensible Authentication Protocol Method for GSM Subscriber Identity, IETF, April 4, 2004
- [GLOBAL PLATFORM] GlobalPlatform Card Specification v2.1.1, GlobalPlatform, March 2003
- [FIPS] FIPS 140-1 and FIPS 140-2 Cryptographic Modules Validation List, National Institute of Standards
- [COMMON CRITERIA] Common Criteria Project
- [EAP-SIM-Handler] EAP-SIM Handler specification V1.1, WLAN Smart Card Consortium, August 1, 2004.
- [EAP-AKA] Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement, IETF, April 5, 2004

9 Authors' Addresses

Pascal Urien

ENST

www.enst.fr

Email: Pascal.Urien@enst.fr

Wouter Habraken

RAAK Technologies

www.raaktechnologies.com

Email: whabraken@raaktechnologies.com

David Flattin

Oberthur Card Systems

www.oberthurcs.com

Email: d.flattin@oberthurcs.com

Herve Ganem

Axalto

www.axalto.com

Email: hganem@axalto.com

10 Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the IETF's procedures with respect to rights in IETF Documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

11 Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

12 Copyright Statement

Copyright (C) The Internet Society (2004). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

13 Acknowledgment

Thanks to Bertrand du Castel, president of the WLAN Smart Card consortium for his valuable comments.