INTERNATIONAL STANDARD

ISO 20828

First edition
2006-07-01

Road vehicles — Security certificate management

Véhicules routiers — Gestion des certificats de sécurité

Reference number
ISO 20828:2006(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 20828 was prepared by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 3, *Electrical and electronic equipment*.

Introduction

Often data transmitted within road vehicles, between road vehicles or from and to road vehicles have to be protected to guarantee their confidentiality and integrity. Cryptography provides excellent means for this kind of protection. Depending on the protection requirements, different schemes may be used. In some situations it is sufficient to lock a data link involving a specific device, and to unlock it only if a second device has sent the correct key in response to an arbitrary seed. The corresponding security access service is specified in various International Standards and is widely used today.

ISO 15764 defines an extended security scheme. It does not just restrict the access to data, but protects the data when transmitted over the data link. Protection is provided against masquerade, replay, eavesdropping, manipulation and repudiation. Before starting the secured data transmission, the data link must be established as a secured link. ISO 15764 provides two methods for this:

a) Both devices participating in the data transmission have a pre-established secret cryptographic key. This key is used to establish the secured link and excludes all third parties not having access to it from participating in the secured link. This method is based on symmetric keys and is applicable to devices with a limited processing power and memory.

b) The secured link may be established between arbitrary devices, if these devices have a private key and a security certificate for the corresponding public key. This method involves asymmetric cryptography requiring a higher amount of processing power and memory at the devices.

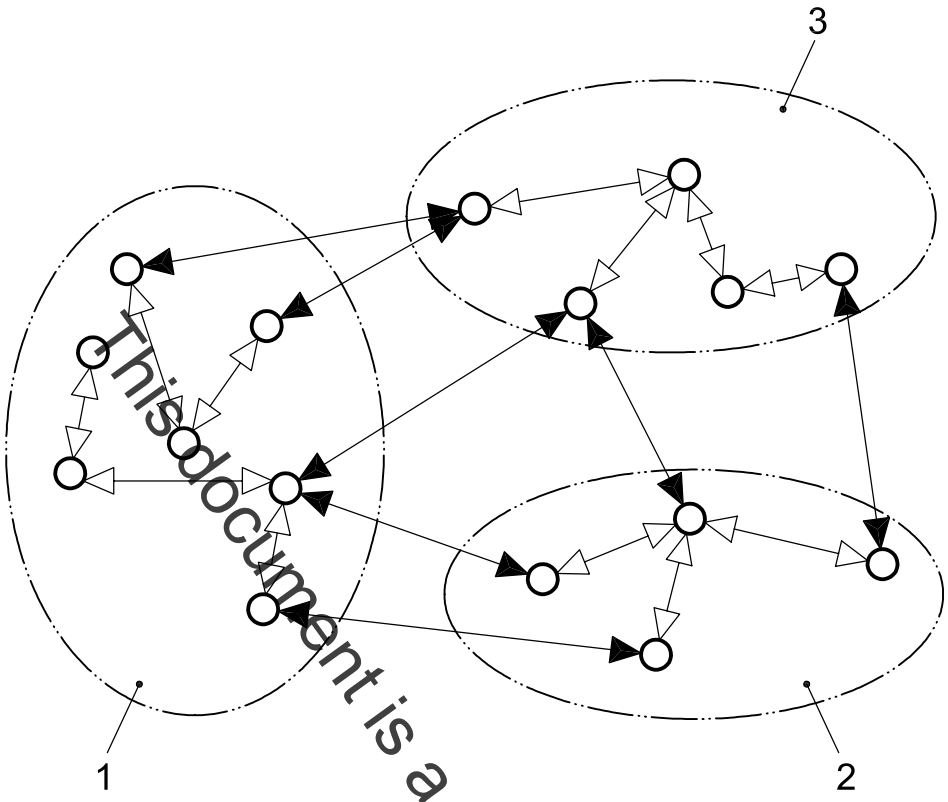
Public keys are cryptographic keys that are publicly available and are linked to a private key, which is kept secret by the device owning it. There are two ways of using a public/private key pair:

a) The device owning the private key may add an electronic signature to data it sends out. This signature is specific for the data sent out and may only be generated with the private key. Both a different data string to be signed and a different private key would lead to a different signature. Any other device possessing the corresponding public key is able to verify the signature and therefore to confirm that the data string originates from the device owning the private key and has not been altered after being sent out.

b) Any device possessing the public key may use it to encrypt data before sending it to the device owning the private key. As the data can only be decrypted with the aid of the private key, no other device is able to correctly interpret the data sent out.

But how does the user of the public key know that it uses the correct one? A malicious third party could send its own public key, pretending it is from a trusted device, and could hope to get access to the secured data transmissions. For each domain of secured data transmissions, there must be an authority (or several of them) deciding which devices can be trusted. This is called Certification Authority. For the trusted devices, it issues security certificates, confirming that the public key is from that device (meaning that the device owns the corresponding private key). The electronic signature of the Certification Authority is attached to the certificate, rendering it unforgeable. As part of the procedure to set up a secured link, the devices involved verify the certificates of each other.

With the second method specified in ISO 15764, a secured link can be established between devices using the public key of the Certification Authority of each other. But in many cases there are different security domains with different authorities responsible to establish trusted devices, and secured links must be established between devices of different domains, not knowing the public keys of the Certification Authorities of the other domain. This International Standard specifies how trust between devices from different security domains is established based on security certificates. In this sense it extends the application range of ISO 15764.



Key

1 security domain 1
2 security domain 2
3 security domain 3
internal secured links covered by ISO 15764
external secured links covered by ISO 20828

Figure 1 — How ISO 20828 extends the application range of ISO 15764

The focus of this International Standard is on the management of certificates. Various security domains based on certificates have already been defined in various contexts. The task of a security certificate management for road vehicles is to give a framework in which such security domains can interact in the sense that secured links can be established from one domain to the other. For instance, there may be specific security domains for different car manufacturers, for public authorities in charge of tachographs or other legislated vehicle components, for telematics service providers, authorized dealers and workshops, emergency task forces and fleet operators. The framework should cover all of them.

When defining this security framework, the following specific requirements of the road vehicle environment have been considered:

— There should be no need for an overall infrastructure to be shared by all security systems. For instance, it can't be expected that shared databases are installed to which the devices involved have access.

— It should be possible to easily integrate existing security systems in the various domains without major modifications.

— The additional security framework should not affect the security of each domain.

— Devices with different security levels are considered. Breaking the security of a device with little protection should not affect the security of other devices.

— It should be possible to use the framework even for devices with limited resources. This means that the provisions requested from the framework should be easy to handle.

The special situation of mobile devices with limited and non-permanent access to communication facilities are considered.

Road vehicles — Security certificate management

1 Scope

This International Standard establishes a uniform practice for the issuing and management of security certificates for use in Public Key Infrastructure applications. Assuming that all entities, intending to set up a secure data exchange to other entities based on private and public keys, are able to provide their own certificate, the certificate management scheme guarantees that the entities will get all additional information needed to establish trust to other entities, from a single source in a simple and unified format. The certificate management is flexible with respect to the relations between Certification Authorities, not requesting any hierarchical structure. It does not prescribe centralized directories or the like, being accessible by all entities involved. With these properties, the management scheme is optimized for applications in the automotive domain.

This International Standard details the role and responsibilities of the Certification Authority relating to certificate issuing and distribution. It specifies how to handle certificate validity and certificate policies. This is the prerequisite for each entity to make sure it can actually trust another entity when intending to exchange data of a specific kind with it.

This International Standard prescribes a Certificate format, which is a special implementation of the well-known X.509 certificate according to ISO/IEC 9594-8. It specifies the structure and use of every certificate component such that it complies with the certificate management established.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 3779, *Road vehicles — Vehicle identification number (VIN) — Content and structure*

ISO 3780, *Road vehicles — World manufacturer identifier (WMI) code*

ISO/IEC 8824-1, *Information technology — Abstract Syntax Notation One (ASN.1) — Part 1: Specification of basic notation*

ISO/IEC 8824-2, *Information technology — Abstract Syntax Notation One (ASN.1) — Part 2: Information object specification*

ISO/IEC 8824-3, *Information technology — Abstract Syntax Notation One (ASN.1) — Part 3: Constraint specification*

ISO/IEC 9594-2, *Information technology — Open Systems Interconnection — Part 2:The Directory: Models*

ISO/IEC 9594-8, *Information technology — Open Systems Interconnection — Part 8: The Directory: Public-key and attribute certificate frameworks*

ISO/IEC 15408-3, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements*

ISO 15764, *Road vehicles — Extended data link security*

IETF RFC 3279, *Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, R. Housley, W. Polk, W. Ford, D. Solo, April 2002*

IETF RFC 3280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, W. Polk, R. Housley, L. Bassham, April 2002*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 9594-8, in ISO 15764 and the following apply.

3.1
certificate
public-key certificate as defined in ISO/IEC 9594-8, including further information as specified in this International Standard

3.2
certificate validity
assignment of one of the two states "valid" or "invalid" to a certificate by its issuer, which only guarantees that the certificate can be used to establish trust between end entities if it is valid

3.3
Certification Authority List
CAL
list maintained by a CA for one of its public keys, the corresponding private key being used to sign certificates, containing information on other CA having issued CA-certificates with this public key being the public key of the subject, and information on these CA-certificates

3.4
certification path
ordered sequence of different CAs, together with their public keys and CA-certificates issued by them and signed with the corresponding private key, in which each public key of the subject in one of these CA-certificates is the public key of the next CA in the sequence

3.5
Certification Path Information (CPI)
information maintained by a CA for one of its public keys, the corresponding private key being used to sign certificates including information on all certification paths starting at that CA with a CA-certificate being signed by that private key, as well as validity information on the CA-certificates in the certification paths and on the certificates issued for end entities by one of the CA in the certification paths and being signed with the private key corresponding to its public key

3.6
confirmation of trust
information accessible without restrictions and allowing an entity to verify that it can trust another entity

3.7
end entity
entity involved in the establishment of a secure data exchange and not installed at a CA

3.8
entity
technical equipment, protected against access by third parties, that is capable to exchange data on a communication link to which third parties may get access

