

DỰ THẢO

TCVN 12854-7:2026

ISO/IEC 29192-7:2019

Xuất bản lần 1

**BẢO MẬT THÔNG TIN - MẬT MÃ HẠNG NHẹ -
PHẦN 7: GIAO THỨC XÁC THỰC QUẢNG BÁ**

Information security - Lightweight cryptography - Part 7:

Broadcast authentication protocols

Mục lục

Lời giới thiệu	5
1 Phạm vi áp dụng	7
2 Tài liệu viện dẫn	7
3 Thuật ngữ và định nghĩa	7
4 Ký hiệu và thuật ngữ viết tắt	9
5 TESLA-RD (Xác thực luồng hiệu quả theo thời gian, chịu lỗi mất gói — Tiết lộ khóa nhanh)	10
5.1 Tổng quan	10
5.2 Khởi tạo	10
5.3 Thiết lập	11
5.4 Gửi thông điệp	11
5.5 Nhận thông điệp	11
5.6 Xác thực khóa	11
5.7 Xác thực thông điệp	11
PHỤ LỤC A (Quy định) Định danh đối tượng	12
Thư mục tài liệu tham khảo	13

TCVN 12854-7:2026

Lời nói đầu

TCVN 12854-7:2026 hoàn toàn tương đương với ISO/IEC 29192-7:2019.

TCVN 12854-7:2026 do Ban Cơ yếu Chính phủ biên soạn, Bộ Quốc phòng đề nghị, Ủy Ban Tiêu chuẩn Đo lường Chất lượng Quốc gia thẩm định, Bộ Khoa học và Công nghệ công bố.

Bộ tiêu chuẩn TCVN 12854 Công nghệ thông tin - Kỹ thuật an toàn - Mật mã hạng nhẹ, gồm 08 phần:

- TCVN 12854-1: 2020 Phần 1: Tổng quan.
- TCVN 12854-2: 2020 Phần 2: Mã khối.
- TCVN 12854-3: 2020 Phần 3: Mã dòng.
- TCVN 12854-4: 2020 Phần 4: Cơ chế sử dụng kỹ thuật phi đối xứng.
- TCVN 12854-5: 2020 Phần 5: Các hàm băm.
- TCVN 12854-6: 2026 Phần 6: Mã xác thực thông điệp (MAC).
- TCVN 12854-7: 2026 Phần 7: Giao thức xác thực quảng bá.
- TCVN 12854-8: 2026 Phần 8: Mã hóa xác thực.

Lời giới thiệu

Nhiều môi trường công nghệ thông tin liên quan đến phương thức truyền tin quảng bá, trong đó một bên gửi giao tiếp với nhiều bên nhận. Việc bảo mật các phương thức truyền tin như vậy là một nhiệm vụ không hề đơn giản. Các giao thức xác thực quảng bá hướng tới việc cho phép bên nhận xác minh tính xác thực của dữ liệu được truyền đi và đảm bảo xác thực thực thể của bên gửi.

Một cách trực diện để đạt được xác thực quảng bá là sử dụng chữ ký số, ví dụ như được mô tả trong bộ tiêu chuẩn TCVN 12855 (ISO/IEC 9796) hoặc TCVN 12214 (ISO/IEC 14888). Tuy nhiên, có những tình huống mà chi phí về mặt truyền thông và tính toán bổ sung của chữ ký số là quá đắt đỏ và không khả thi, chẳng hạn như trong trường hợp vệ tinh truyền tín hiệu quảng bá xuống Trái đất.

Tiêu chuẩn này quy định các giao thức xác thực quảng bá hạng nhẹ, mang lại chi phí triển khai thấp hơn đáng kể so với việc sử dụng chữ ký số như một giải pháp cho việc xác thực truyền tin quảng bá.

Bảo mật thông tin - Mật mã hạng nhẹ - Phần 7: Giao thức xác thực quảng bá

Information security - Lightweight cryptography - Part 7: Broadcast authentication protocols

1 Phạm vi áp dụng

Tiêu chuẩn này quy định các giao thức xác thực quảng bá, là các giao thức cung cấp tính toàn vẹn dữ liệu và xác thực thực thể trong môi trường quảng bá, tức là môi trường có một bên gửi truyền thông điệp đến nhiều bên nhận. Để thực hiện xác thực thực thể, cần phải có một cơ sở hạ tầng đã tồn tại từ trước nhằm liên kết bên gửi với một bí mật mật mã. Việc thiết lập cơ sở hạ tầng như vậy nằm ngoài phạm vi của tiêu chuẩn này.

2 Tài liệu viện dẫn

Các tài liệu dẫn chiếu sau đây là bộ phận không thể tách rời và cấu thành một phần hoặc toàn bộ yêu cầu của tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi, bổ sung (nếu có).

TCVN 11495 (ISO/IEC 9797 tất cả các phần) Công nghệ thông tin - Các kỹ thuật an toàn - Mã xác thực thông điệp (MAC)

TCVN 11816-1:2017 (ISO/IEC 10118 tất cả các phần) Công nghệ thông tin - Các kỹ thuật an toàn - Hàm băm

TCVN 12854-1 (ISO/IEC 29192-1) Công nghệ thông tin - Kỹ thuật an toàn - Mật mã hạng nhẹ -Phần 1: Tổng quan

TCVN 12854-5 (ISO/IEC 29192-5) Công nghệ thông tin - Kỹ thuật an toàn - Mật mã hạng nhẹ - Phần 5: Các hàm băm

TCVN 12854-6 (ISO/IEC 29192-6) Công nghệ thông tin - Mật mã hạng nhẹ - Phần 6: Mã xác thực thông điệp (MAC)

3 Thuật ngữ và định nghĩa

Đối với mục đích của tiêu chuẩn này, các thuật ngữ và định nghĩa được nêu trong tiêu chuẩn TCVN 12854-1 (ISO/IEC 29192-1) và các thuật ngữ dưới đây được áp dụng:

3.1

Quảng bá (broadcast)

Phương thức truyền tin, trong đó thông tin bắt nguồn từ một bên gửi (3.11) được phân phối tới một nhóm bên nhận (3.9).

3.2

Tính toàn vẹn dữ liệu (data integrity)

Đặc tính bảo đảm dữ liệu không bị thay đổi hoặc phá hủy trái phép.

TCVN 12854-7:2026

[Nguồn TCVN 11495-1:2016, 3.4].

3.3

Hàm băm kháng va chạm (collision-resistant hash-function)

Hàm băm (3.4) thỏa mãn tính chất sau: về mặt tính toán, không khả thi để tìm được bất kỳ hai đầu vào phân biệt nào cùng ánh xạ tới một đầu ra.

Chú thích: Tính khả thi về mặt tính toán phụ thuộc vào các yêu cầu bảo mật và môi trường cụ thể.

3.4

Hàm băm (hash-function)

Hàm ánh xạ các chuỗi bit thành các chuỗi bit có độ dài cố định, thỏa mãn hai tính chất sau đây:

— Đối với một đầu ra cho trước, về mặt tính toán là không khả thi để tìm ra một đầu vào ánh xạ tới đầu ra đó;

— Đối với một đầu vào cho trước, về mặt tính toán là không khả thi để tìm ra một đầu vào thứ hai ánh xạ tới cùng một đầu ra.

Chú thích: Tính khả thi về mặt tính toán phụ thuộc vào các yêu cầu bảo mật và môi trường cụ thể.

3.5

Khóa (key)

Chuỗi các ký hiệu điều khiển hoạt động của một phép biến đổi mật mã (ví dụ: mã hóa, giải mã, tính toán hàm kiểm tra mật mã, tạo chữ ký hoặc xác thực chữ ký).

[Nguồn TCVN 11367-3:2016, 2.4 (ISO/IEC 18033-3:2010, 2.4), Đã sửa đổi - Giữa các dấu ngoặc, các từ phía sau chữ "giải mã" đã được bổ sung].

3.6

Khóa thuật toán MAC (MAC algorithm key)

Khóa điều khiển hoạt động của thuật toán MAC.

[Nguồn TCVN 11495-1:2016, 3.8 (ISO/IEC 9797-1:2011, 3.8)].

3.7

Mã xác thực thông điệp (Message Authentication Code)

MAC

Chuỗi bit là đầu ra của một thuật toán MAC.

Chú thích: MAC đôi khi được gọi là giá trị kiểm tra mật mã (xem ví dụ tại TCVN 9696-2 (ISO 7498-2)).

3.8

Thuật toán mã xác thực thông điệp (Message Authentication Code algorithm)

MAC algorithm

Thuật toán dùng để tính toán một hàm ánh xạ các chuỗi bit và một khóa bí mật thành các chuỗi bit có độ dài cố định, thỏa mãn hai tính chất sau:

— Với bất kỳ khóa nào và bất kỳ chuỗi đầu vào nào, hàm này đều có thể được tính toán một cách hiệu quả;

— Đối với bất kỳ khóa cố định nào và khi không có tri thức trước về khóa, về mặt tính toán là không khả thi để tính toán giá trị hàm trên bất kỳ chuỗi đầu vào mới nào, ngay cả khi biết tập hợp các chuỗi đầu vào và các giá trị hàm tương ứng, trong đó giá trị của chuỗi đầu vào thứ i có thể đã được chọn sau khi quan sát giá trị của $i - 1$ hàm trước đó (đối với các số nguyên $i > 1$).

Chú thích 1: Thuật toán MAC đôi khi được gọi là hàm kiểm tra mật mã (xem ví dụ tại TCVN 9696-2 (ISO 7498-2)).

Chú thích 2: Tính khả thi về mặt tính toán phụ thuộc vào các yêu cầu bảo mật và môi trường cụ thể của người dùng.

[Nguồn TCVN 11495-1:2016, 3.10 (ISO/IEC 9797-1:2011, 3.10)]

3.9

Bên nhận (receiver)

Thực thể nhận thông tin từ bên gửi (3.11), yêu cầu tính toán vẹn dữ liệu và xác thực thực thể (3.10).

3.10

Xác thực thực thể (entity authentication)

Sự xác nhận rằng một thực thể chính là thực thể đã được tuyên bố.

[Nguồn TCVN 11817:2017, 3.14 (ISO/IEC 9798-1:2010, 3.14)]

3.11

Bên gửi (sender)

Thực thể tạo các thông điệp để phát quảng bá (3.1).

3.12

Chuỗi khóa (chain of keys)

Chuỗi khóa được tạo ra bằng cách áp dụng hàm băm kháng va chạm (3.3) vào một khóa (3.5) và sau đó liên tục áp dụng hàm băm kháng va chạm vào đầu ra của lần thực hiện trước đó.

4 Ký hiệu và thuật ngữ viết tắt

$F(X)$	Đầu ra của hàm băm F khi được áp dụng cho dữ liệu X , được cắt ngắn đến độ dài cần thiết cho các khóa được thuật toán MAC sử dụng
$MAC(K, M)$	Đầu ra của thuật toán MAC với đầu vào là khóa K của thuật toán MAC và thông điệp M
$X Y$	Phép nối các mục dữ liệu X và Y theo thứ tự được quy định
CHÚ THÍCH 1 : Đối với các chuỗi X , K , M , Y có độ dài tùy ý	
D	Độ dài của mỗi khoảng thời gian
d	Độ trễ giữa việc truyền MAC và việc tiết lộ khóa, được đo bằng đơn vị D

TCVN 12854-7:2026

N	Độ dài của một chuỗi khóa
α	Một giá trị được sử dụng trong quá trình tạo chuỗi khóa nhằm ngăn chặn các cuộc tấn công đánh đổi thời gian-bộ nhớ
L	Độ dài của α
i, j	Các khoảng thời gian
$ i $	Số lượng bit được sử dụng để biểu diễn khoảng thời gian thứ i . Cách biểu diễn này phải là duy nhất trong suốt vòng đời của hệ thống. Bất cứ khi nào i được sử dụng dưới dạng chuỗi bit, nó phải được chuyển đổi theo mô tả của hàm chuyển đổi I2BS từ tài liệu WG2 SD 7, 4.3.9 (phiên bản thứ 2).
M_i	Thông điệp được gửi trong khoảng thời gian thứ i

CHÚ THÍCH 2 : D , d , N , L và $|i|$ được gọi là các 'tham số hệ thống' và được quyết định cũng như công khai trước khi khởi tạo hệ thống

5 TESLA-RD (Xác thực luồng hiệu quả theo thời gian, chịu lỗi mất gói — Tiết lộ khóa nhanh)

5.1 Tổng quan

Giao thức TESLA-RD sử dụng một thuật toán MAC và một hàm băm kháng va chạm. Thuật toán MAC phải thuộc tiêu chuẩn TCVN 11495 (ISO/IEC 9797 (tất cả các phần)) hoặc TCVN 12854-6 (ISO/IEC 29192-6), và hàm băm kháng va chạm phải thuộc tiêu chuẩn TCVN 11816 (ISO/IEC 10118 (tất cả các phần)) hoặc TCVN 12854-5 (ISO/IEC 29192-5).

Phụ lục A xác định các mã định danh đối tượng sẽ được sử dụng để nhận diện các thuật toán được quy định trong tiêu chuẩn này.

CHÚ THÍCH 1: Việc lựa chọn các thuật toán MAC và hàm băm kháng va chạm không thuộc loại mật mã hạng nhẹ có thể làm giảm lợi ích của việc sử dụng TESLA-RD trong các môi trường bị hạn chế về tài nguyên.

Bên gửi và tất cả các bên nhận phải có một đồng hồ nội bộ. Thời gian của bên gửi theo đồng hồ nội bộ của nó được ký hiệu là T_s . Thời gian của một bên nhận theo đồng hồ nội bộ của nó được ký hiệu là T_r . Chênh lệch giữa thời gian của bên gửi, T_s , và thời gian của bên nhận, T_r , phải bị chặn trên trong suốt vòng đời của hệ thống bởi một giá trị ε cố định và đã biết, tức là $|T_s - T_r| < \varepsilon$.

CHÚ THÍCH 2: Cơ chế vận hành bên trong của các đồng hồ nội bộ, cũng như quy trình về cách đạt được đồng bộ hóa thời gian, nằm ngoài phạm vi của tiêu chuẩn này.

Thời gian phải được chia thành các khoảng có độ dài cố định D . Mỗi khoảng thời gian được liên kết với một khóa (3.5) từ chuỗi khóa (3.12) hiện đang có hiệu lực. Khoảng thời gian thứ nhất được liên kết với khóa cuối cùng, khoảng thời gian thứ hai được liên kết với khóa áp chót, v.v. Vào cuối mỗi khoảng thời gian, một gói tin có thể được phát quảng bá. Gói tin phải được xử lý bằng một thuật toán MAC sử dụng khóa được liên kết với khoảng thời gian đó, và khóa sẽ được phát quảng bá sau một độ trễ là d khoảng thời gian.

CHÚ THÍCH 3: Tích số của các tham số D và d là độ trễ giữa việc nhận thông điệp và việc xác thực thông điệp đó.

Sau khi N khóa đã được phát quảng bá, chuỗi khóa sẽ cạn kiệt và một chuỗi mới phải được sử dụng.

5.2 Khởi tạo

Trong giai đoạn khởi tạo, bên gửi phải chọn một thuật toán MAC (3.8) và một hàm băm kháng va chạm (3.3), đồng thời quyết định các tham số hệ thống sau: D , d và N . Mọi tham số này phải được truyền tới bên nhận theo quy trình bảo mật nhằm xác thực thực thể bên gửi và bảo vệ tính toàn vẹn dữ liệu.

5.3 Thiết lập

Bên gửi phải tính toán một chuỗi khóa bằng cách trước tiên tạo ra giá trị α và một khóa thuật toán MAC K_N ngẫu nhiên đều. Sau đó, bên gửi phải sử dụng hàm băm kháng va chạm để tính toán các khóa thuật toán MAC $K_i = F(K_{i+1} || i || \alpha)$, với $i = N-1, N-2, \dots, 0$. Khóa K_0 phải được phân phối đến các bên nhận theo quy trình bảo mật nhằm xác thực thực thể bên gửi và bảo vệ tính toàn vẹn dữ liệu. Giá trị α cũng phải được phân phối tương tự.

Việc phân phối khóa K_0 , ví dụ, có thể được bảo mật bằng các chữ ký số hoặc bằng một cơ chế khởi tạo khác của giao thức TESLA-RD với tham số D và d lớn hơn.

Độ dài của α có thể được đặt bằng không. Tuy nhiên, để ngăn chặn các cuộc tấn công đánh đổi thời gian-bộ nhớ, α nên có độ dài khác không nếu K_0 được công bố trước thời điểm bắt đầu của chuỗi khóa khá lâu.

5.4 Gửi thông điệp

Trong khoảng thời gian thứ i , với $i = 1, \dots, N$, bên gửi phát quảng bá thông điệp M_i đã được xử lý bằng thuật toán MAC sử dụng khóa K_i . Bên gửi cũng phát quảng bá chỉ số khoảng thời gian i và khóa K_{i-d} liên kết với khoảng thời gian thứ $(i-d)$. Một gói tin được truyền đi trong khoảng thời gian thứ i được xây dựng theo Công thức (1):

$$P_i = M_i || i || \text{MAC}(K_i, M_i) || K_{i-d} \quad (1)$$

5.5 Nhận thông điệp

Khi bên nhận nhận được một gói tin P_i với chỉ số khoảng thời gian là i , trước tiên họ phải kiểm tra xem thông điệp có được nhận đúng thời điểm T_r hay không, sao cho $T_r < i - d$. Nếu thỏa mãn điều kiện này, gói tin sẽ được lưu trữ để xử lý sau. Ngược lại, gói tin đó sẽ bị loại bỏ.

5.6 Xác thực khóa

Sau một độ trễ là d gói tin, một gói tin P_{i+d} sẽ được phát hành, trong đó bao gồm khóa K_i . Sau đó, khóa K_i sẽ được xác thực dựa trên một khóa K_j đã được xác thực trước đó, với $j < i$, bằng cách tính toán theo Công thức (2):

$$K'_j = F(\dots(F(F(K_j || i-1 || \alpha) || i-2 || \alpha) \dots) || j || \alpha) \quad (2)$$

và kiểm tra xem $K'_j = K_j$ có thỏa mãn hay không. Nếu hai giá trị này khớp nhau, K_i sẽ được chấp nhận là một khóa hợp lệ. Ngược lại, nó sẽ bị loại bỏ.

Tùy thuộc vào ứng dụng, một khi K_i được chấp nhận là hợp lệ, bên nhận có thể chọn thay thế K_j bằng K_i để giảm bớt khối lượng tính toán cần thiết cho việc xác thực khóa tiếp theo.

5.7 Xác thực thông điệp

Sau khi khóa K_i đã được xác thực, thông điệp M_i và giá trị $\text{MAC}(M_i, K_i)$ của nó sẽ được lấy ra từ gói tin P_i đã được lưu trữ trước đó. Một giá trị MAC giả định của M_i sẽ được tính toán bằng cách sử dụng thuật toán MAC, thông điệp M_i đã trích xuất, và khóa K_i đã xác thực; sau đó giá trị này được so sánh với giá trị MAC đã lưu trữ. Nếu chúng bằng nhau, thông điệp sẽ được chấp nhận là hợp lệ. Ngược lại, nó sẽ bị từ chối.

PHỤ LỤC A
(Quy định)
Định danh đối tượng

Phụ lục này liệt kê các mã định danh đối tượng được gán cho các thuật toán được quy định trong tiêu chuẩn này

```
--
-- Object identifiers of ISO/IEC 29192-7
--
LightweightCryptography-7 {
    iso(1)                standard(0)                lightweight-
        cryptography(29192)    part7(7)    asn1-module(0)
        algorithm-object-identifiers(0) }

DEFINITIONS    EXPLICIT    TAGS    ::=

BEGIN EXPORTS ALL;

IMPORTS ;

OID ::= OBJECT IDENTIFIER -- Alias

-- Synonyms --

is29192-7 OID ::= {
    iso(1) standard(0) lightweight-cryptography(29192) part7(7) }

-- Assignments --

id-tesla OID ::= { is29192-7 tesla(1) }

LightweightCryptographyIdentifier ::=
    ProtocolIdentifier    {{ BroadcastAuthenticationProtocols    }}

BroadcastAuthenticationProtocols PROTOCOL ::= {

    ... -- Expect additional protocol objects --
}

PROTOCOL ::= CLASS {
    &id    OBJECT IDENTIFIER    UNIQUE,
    &Type    OPTIONAL
}
    WITH SYNTAX { OID &id [ PARMS &Type ] }

ProtocolIdentifier { PROTOCOL:IOSet } ::=
    SEQUENCE    {
        protocol
            PROTOCOL.&id({IOSet}),
        parameters    PROTOCOL.&Type({IOSet}{@protocol})    OPTIONAL
    }

END -- LightweightCryptography-7 --
```

Thư mục tài liệu tham khảo

- [1] TCVN 9696-2 (ISO/IEC 7498-2) Công nghệ thông tin – Liên kết hệ thống mở - Mô hình tham chiếu cơ sở - Phần 2: Kiến trúc an ninh.
 - [2] TCVN 12855 (ISO/IEC 9796 tất cả các phần) Công nghệ thông tin - Các kỹ thuật an toàn - Lược đồ chữ ký số cho khôi phục thông điệp.
 - [3] TCVN 11817-1(ISO/IEC 9798-1) Công nghệ thông tin - Các kỹ thuật an toàn - Xác thực thực thể - Phần 1: Tổng quan.
 - [4] TCVN 12214(ISO/IEC 14888 (tất cả các phần)), Công nghệ thông tin - Các kỹ thuật an toàn - Chữ ký số kèm phụ lục.
 - [5] TCVN 11367-3 (ISO/IEC 18033-3) Công nghệ thông tin – Các kỹ thuật an toàn – Thuật toán mật mã – Phần 3: Mã khối.
 - [6] PeRRlg A., Canettl R., TygaR J.D., Song Dawn, Efficient authentication and signing of multicast streams over lossy channels. Proceedings of the 2000 IEEE Symposium on Security and Privacy, May 2000, pp. 56-73
 - [7] PeRRlg Adrian, Canettl Ran, TygaR J.D, Song Dawn, BRISCoE B., Timed efficient stream loss-tolerant authentication (TESLA): multicast source authentication transform introduction. RFC 4082.
-