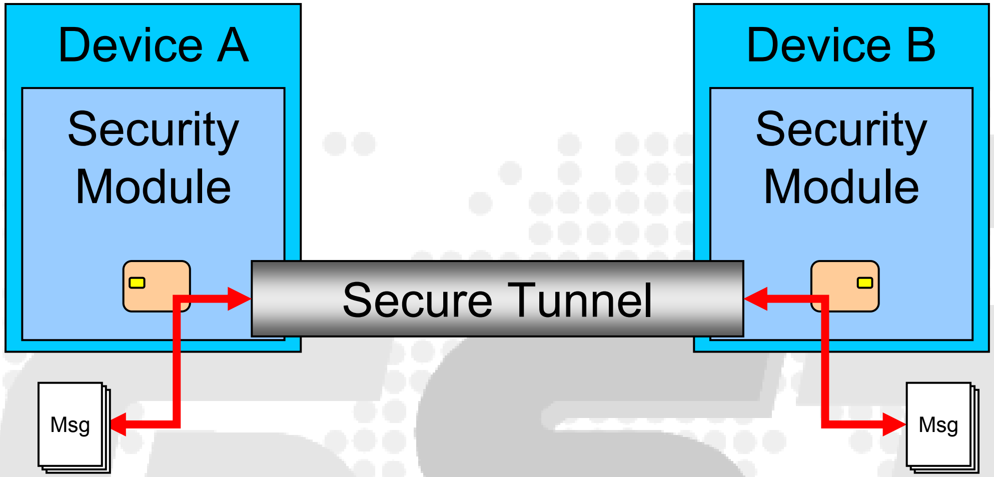
Overview presentation on GST SECurity aspects

Robert Maier, Danny De Cock
{Robert.Maier, Danny.DeCock}@esat.kuleuven.be

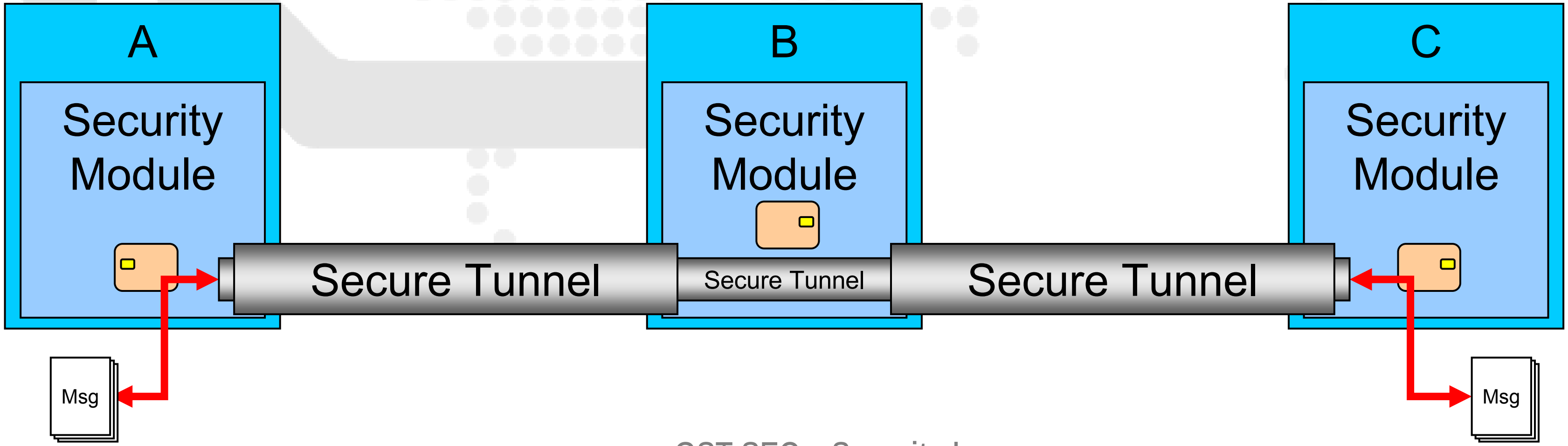
Department of Electrical Engineering ESAT/COSIC
Kasteelpark Arenberg 10
B-3001 Heverlee
Belgium

Presented By Myself

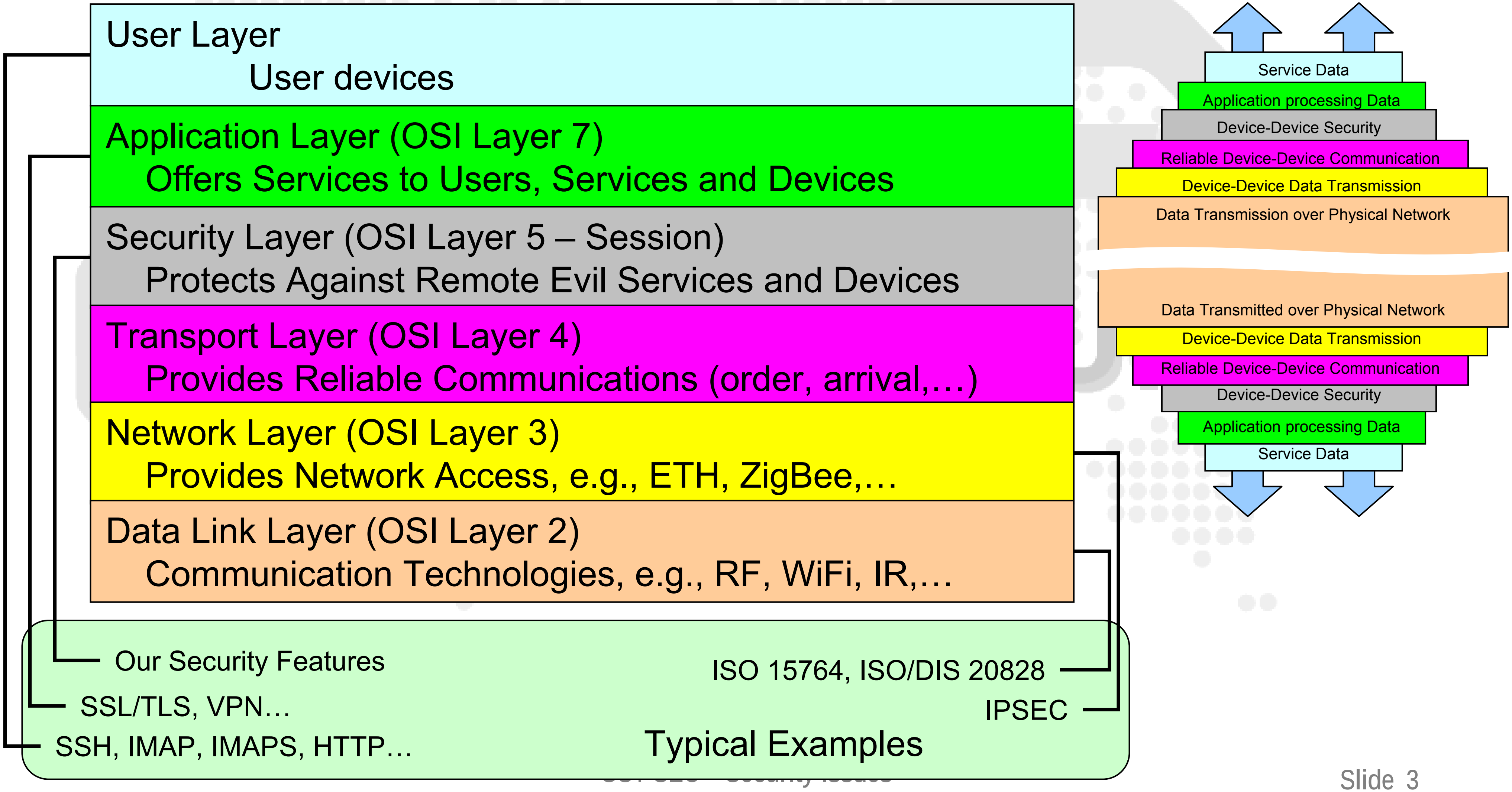
Point-to-Point & End-to-End Communications



Most generic situation:
All secure communication is Point-to-Point
End-to-End secure communications is a Point-to-Point secure communications where the Points may be not directly connected



Protocol Stacks View



User Layer
User devices

Application Layer (OSI Layer 7)
Offers Services to Users, Services and Devices

Security Layer (OSI Layer 5 – Session)
Protects Against Remote Evil Services and Devices

Transport Layer (OSI Layer 4)
Provides Reliable Communications (order, arrival,…)

Network Layer (OSI Layer 3)
Provides Network Access, e.g., ETH, ZigBee,…

Data Link Layer (OSI Layer 2)
Communication Technologies, e.g., RF, WiFi, IR,…

Our Security Features

SSL/TLS, VPN…

SSH, IMAP, IMAPS, HTTP…

ISO 15764, ISO/DIS 20828

IPSEC

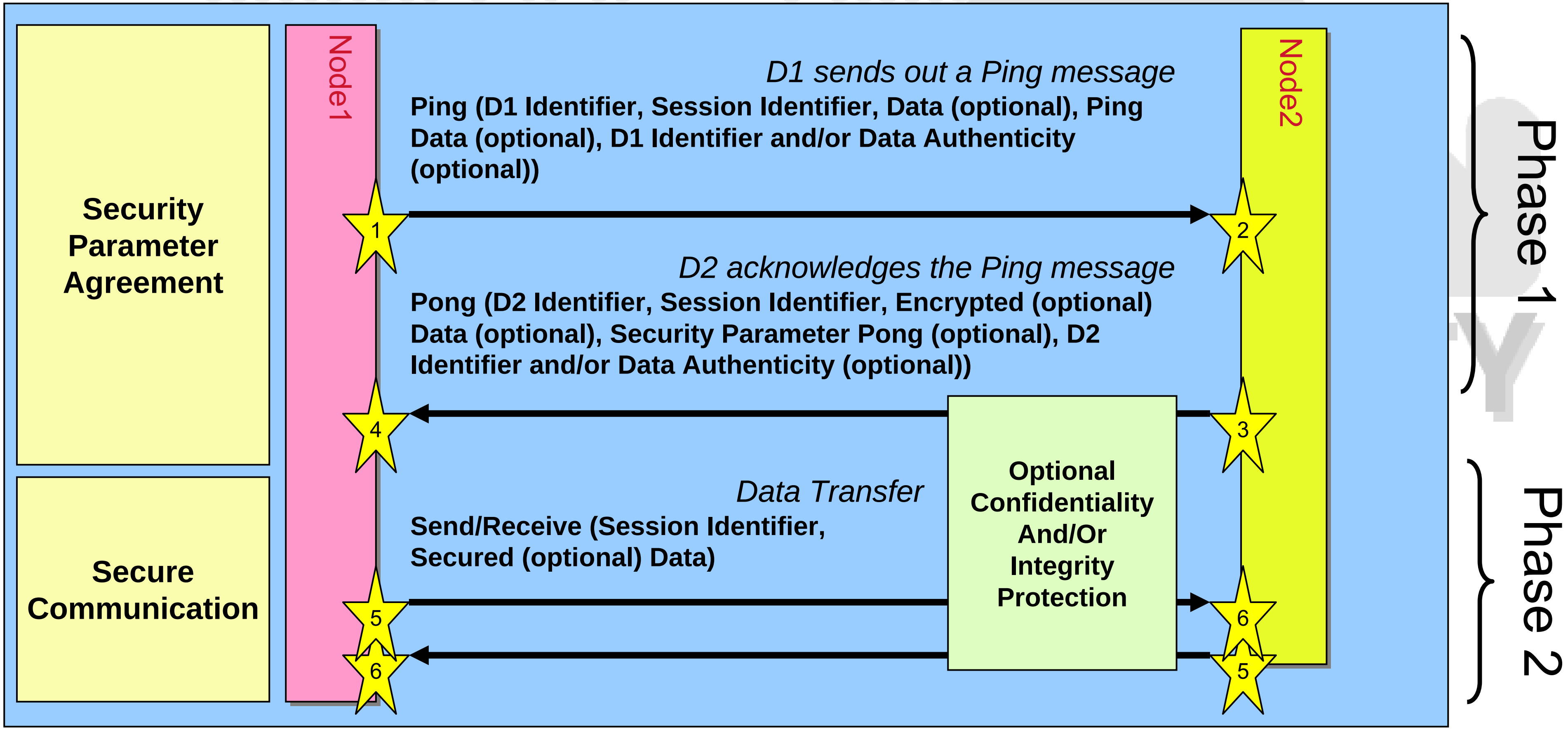
Typical Examples

Service Data
Application processing Data
Device-Device Security
Reliable Device-Device Communication
Device-Device Data Transmission
Data Transmission over Physical Network
Data Transmitted over Physical Network
Device-Device Data Transmission
Reliable Device-Device Communication
Device-Device Security
Application processing Data
Service Data

Secure Communications: 2 Phases

- Phase 1 – Initialization of a secure communications session
  - What?
    - Setting up shared key material for confidentiality and integrity protection
    - Mutual authentication of communicating parties
  - How?
    - Ping Pong: Authenticated Key Agreement based on Diffie-Hellman
- Phase 2 – Using the secure communications session
  - Send/Receive using shared key material established with the Ping Pong

Secure Communications Key Establishment Overview


Security Parameter Agreement
Secure Communication
Node1
Node2
Phase 1
Phase 2
1
2
3
4
5
6
6
5
Optional Confidentiality And/Or Integrity Protection

D1 sends out a Ping message

Ping (D1 Identifier, Session Identifier, Data (optional), Ping Data (optional), D1 Identifier and/or Data Authenticity (optional))

D2 acknowledges the Ping message

Pong (D2 Identifier, Session Identifier, Encrypted (optional) Data (optional), Security Parameter Pong (optional), D2 Identifier and/or Data Authenticity (optional))

Data Transfer

Send/Receive (Session Identifier, Secured (optional) Data)

Secure Communications

Ping

1

Ping message sent from D1 to D2

- Computes secret *x*
- Calculates α^x
- Authenticates $\{data_1||\alpha^x\}$

D1 Broadcasts the Ping message

- Broadcast of Authenticated $(data_1||\alpha^x)$

2

D2 Receives a Ping message

- Checks Authenticated $(data_1||\alpha^x)$
- Processes $data_1$

Pong

4

D1 Receives a Pong message

- Checks Authenticated $(E_K(data_2)||\alpha^y)$
- Calculates $K= (\alpha^y)^x$
- Decrypts $E_K(data_2)$
- Processes $data_2$

3

D2 Prepares a Pong message for D1

- Computes secret y
- Calculates α^y
- Calculates $K= (\alpha^x)^y$
- Encrypts data: $E_K(data_2)$
- Authenticates $\{E_K(data_2)||\alpha^y\}$

D2 Broadcasts Pong message for D1

- Broadcast of Authenticated $(E_K(data_2)||\alpha^y)$

Usage

5

D1 Prepares Secure Data Transfer

- Encrypts $E_K(data_3)$
- Authenticates $E_K(data_3)$

D1 Broadcasts Secured Data Transfer message for D2

- Broadcast of Authenticated $(E_K(data_3))$

6

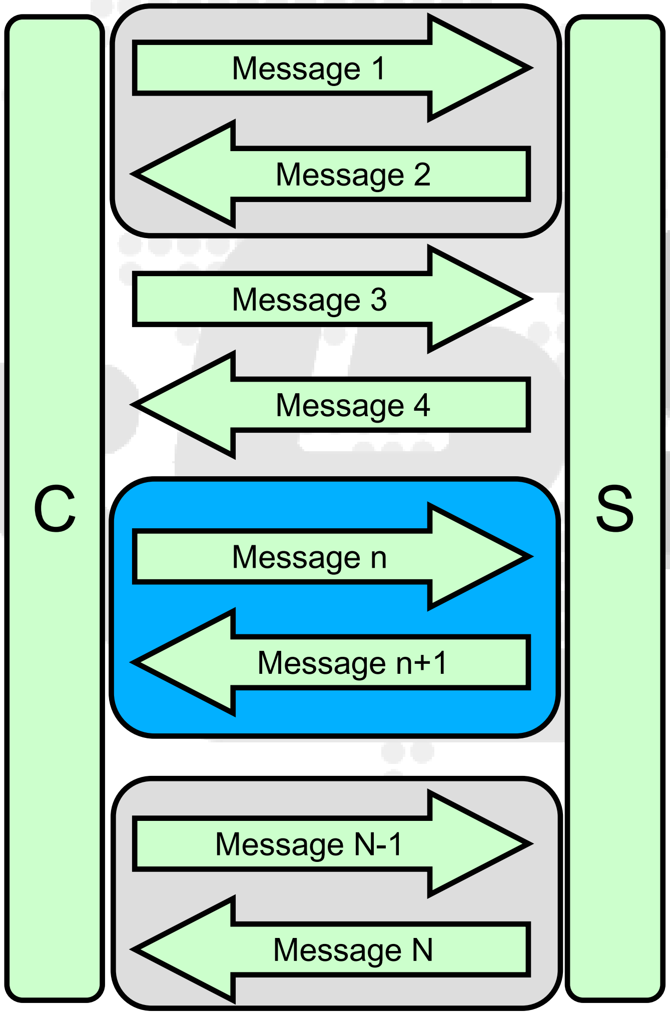
D2 Receives a Secured Data Transfer message

- Checks Authenticated $(E_K(data_3))$

D2 Decrypts the information within a session with D1

- Decrypts $E_K(data_3)$

ISO 15764 – Protocol overview



Secured Link Set-up Request (optional)

Secured Link Set-up Response (optional)

First Secured Data Transmission Request

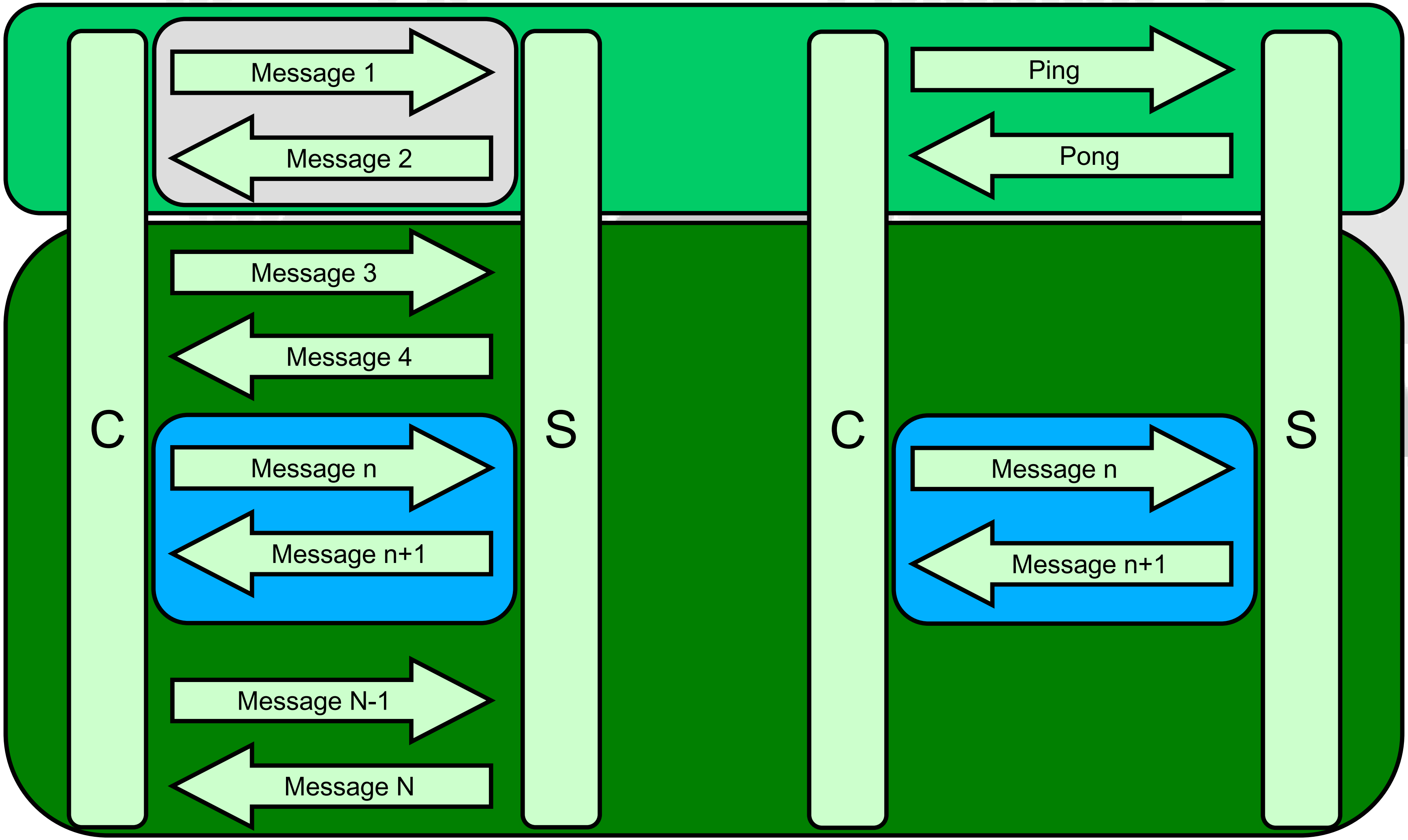
First Secured Data Transmission Response

Further Secured Data Transmission

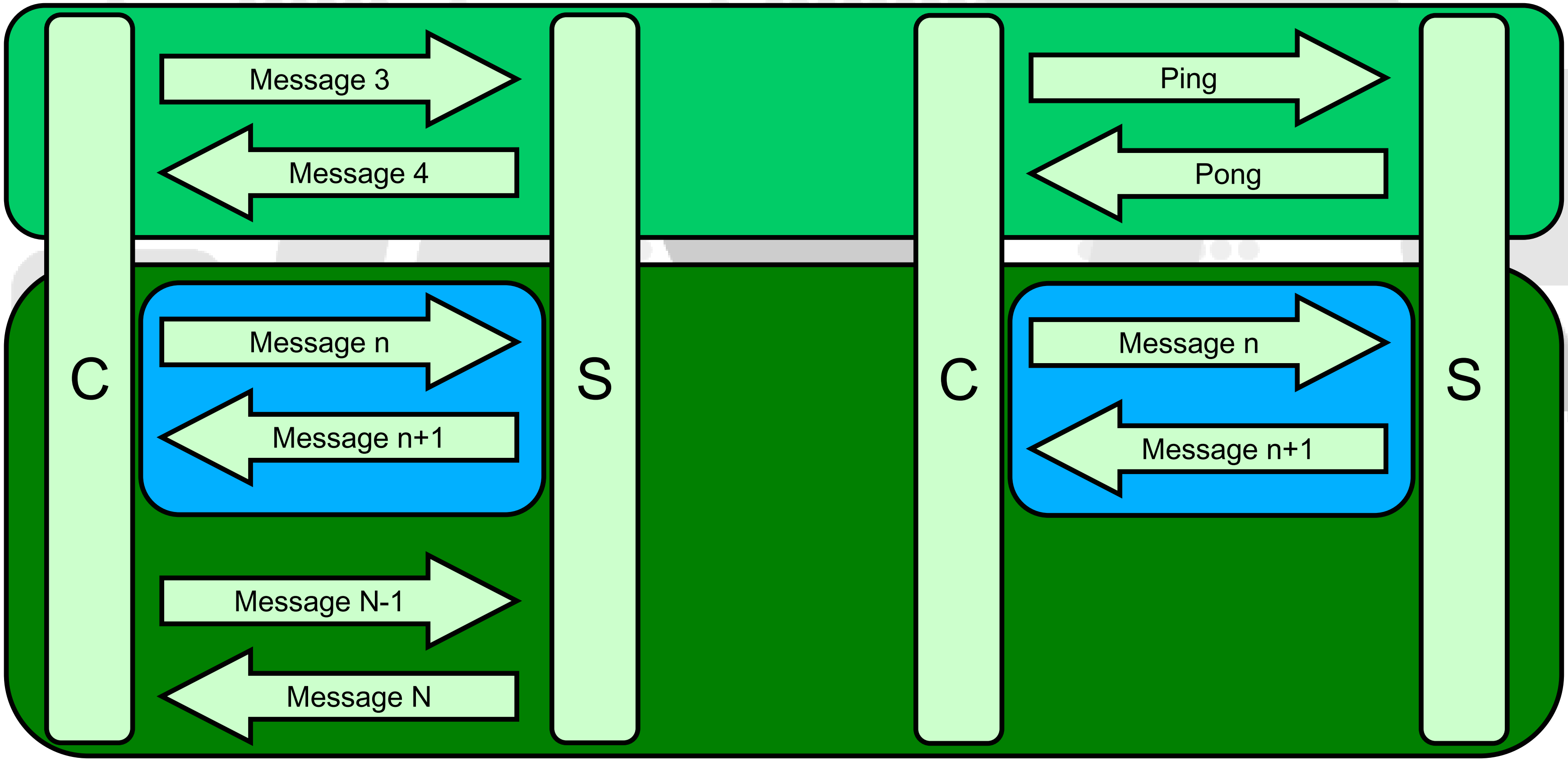
Requests and Responses

Message Sequence Termination (optional)

ISO 15764 compared to GST-SEC ~ nodes never met before ~



ISO 15764 compared to GST-SEC
~ nodes share security data ~



Secure Communications

Message and Data Formats

Message Details – Ping Message

Ping message

Authenticated Data						
Mandatory	Mandatory	Optional	Initialization	Mandatory	Suitable	Mandatory
Message Type	Session Identifier	Destination Address	Ping Data	Security Overhead	Application Data	Authenticity Proof

Ping

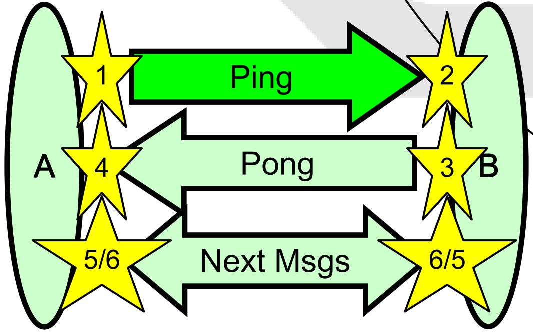
Contains the information from the sender if it does not need to be confidentially protected

Includes the Sender certificate (if no privacy issues), Preferred cryptographic settings

Initialization data to agree on session keys

May refer to the intended destination of the information

Refers to the new session keys initiated with this message and to the credentials of the sender and destination of this new session



🟪 Application Related

🟧 Confidentiality Related

🟩 Authentication Related

🟦 Communication Session Related

🟥 Optionality

Message Details – Pong Message

Pong message

				Encrypted Data				
Authenticated Data								
Mandatory	Mandatory	Optional	Initialization	Mandatory		Suitable	Mandatory	Mandatory
Message Type	Session Identifier	Destination Address	Pong Data	Security Overhead		Application Data	Authenticity Proof	Encryption Padding

Pong

Answer to the initialization data to agree on session keys

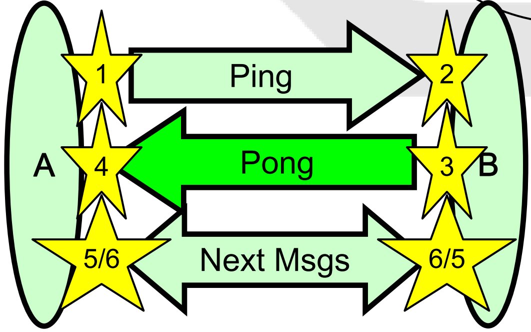
Contains sender's information which must be confidentially protected

May refer to the intended destination of the information

Refers to the session initiated by the previous Ping message

Includes the encryption IV, Sender certificate, and the chosen cryptographic settings

Makes the length of the plaintext data a multiple of the block cipher's block length



🟪 Application Related

🟧 Confidentiality Related

🟩 Authentication Related

🟦 Communication Session Related

🟥 Optionality

Message Details – Insecure Message

No cryptographic mechanisms are used to protect the message

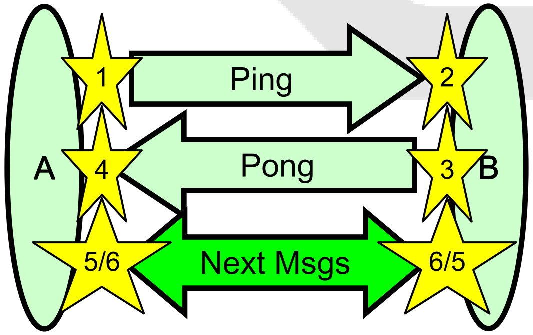
Mandatory	Optional	Optional	Optional	Suitable
Message Type	Session Identifier	Destination Address	Sender Address	Application Data

Message Type: Insecure

Destination Address: May refer to the intended destination of the information

Session Identifier: May refer to the session keys and credentials known by the intended destination

Sender Address: May refer to the sender of the information



Application Related

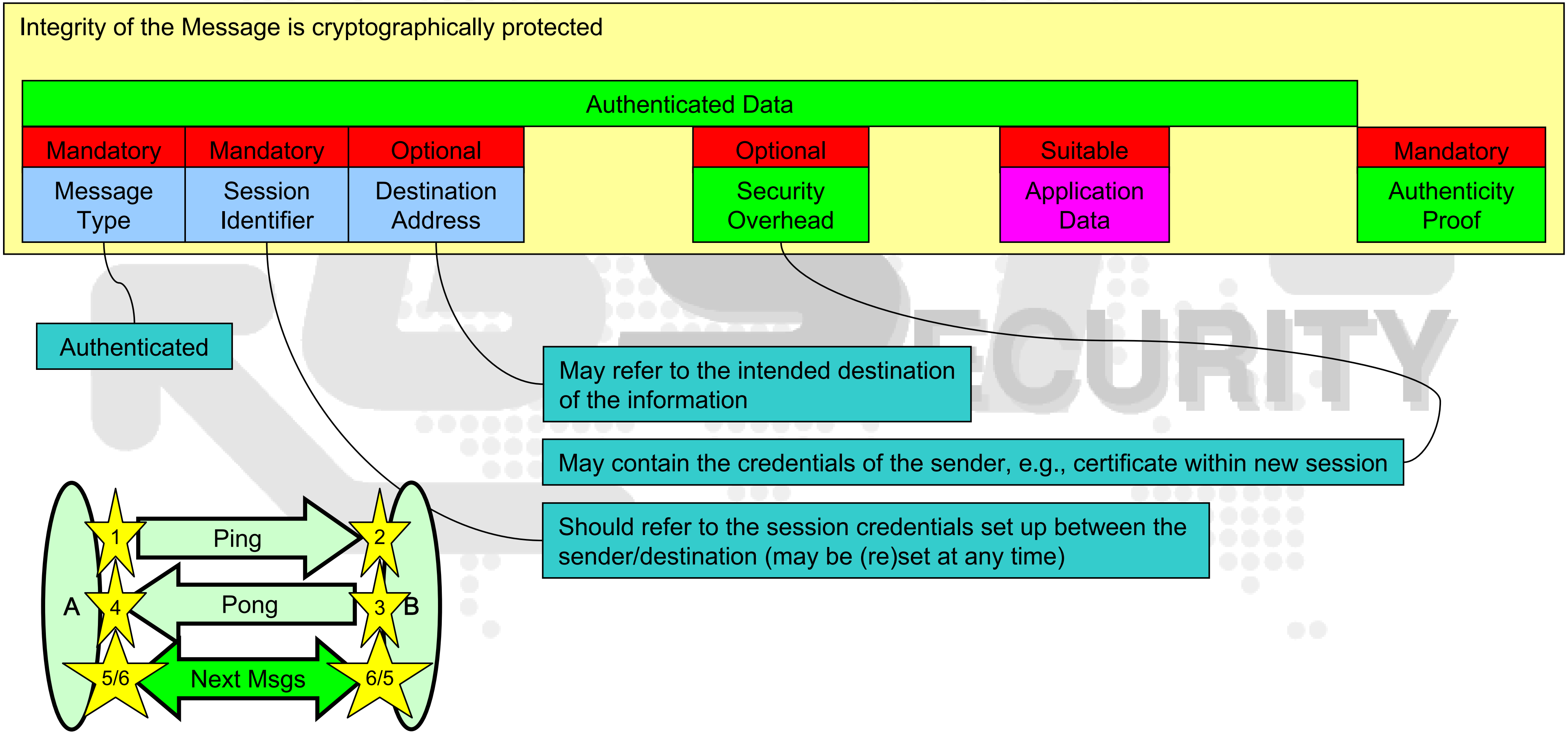
Confidentiality Related

Authentication Related

Communication Session Related

Optionality

Message Details – Authenticated Message



Integrity of the Message is cryptographically protected

Authenticated Data

Mandatory	Mandatory	Optional	Optional	Suitable	Mandatory
Message Type	Session Identifier	Destination Address	Security Overhead	Application Data	Authenticity Proof

Authenticated

May refer to the intended destination of the information

May contain the credentials of the sender, e.g., certificate within new session

Should refer to the session credentials set up between the sender/destination (may be (re)set at any time)

🟪 Application Related

🟧 Confidentiality Related

🟩 Authentication Related

🟦 Communication Session Related

🟥 Optionality

Message Details – Confidential Message

Confidentiality of the message is cryptographically protected

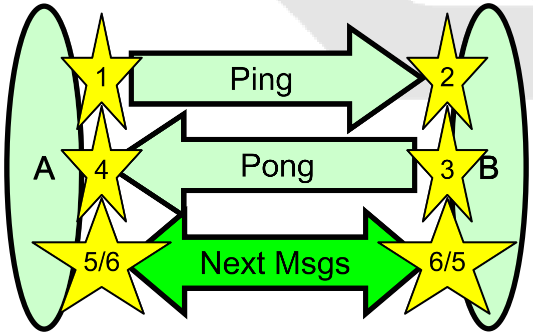
				Encrypted	
Mandatory	Mandatory	Optional	Mandatory	Suitable	Mandatory
Message Type	Session Identifier	Destination Address	Security Overhead	Application Data	Encryption Padding

Confidential

May refer to the intended destination of the information

Encryption IV, Ping sender's certificate (only once, only if privacy issues

Should refer to the session keys and credentials agreed on between the sender and destination during an earlier ping pong



Notes:

1. A confidential message must have been preceded by a ping pong
2. This mode is **not** recommended – the integrity of the IV should be protected

Application Related

Confidentiality Related

Authentication Related

Communication Session Related

Optionality

Message Details – Secure Message (Type 1)

Authenticated data is encrypted

Encrypted Data

Authenticated Data

Mandatory	Mandatory	Optional	Mandatory	Suitable	Mandatory	Mandatory
Message Type	Session Identifier	Destination Address	Security Overhead	Application Data	Authenticity Proof	Encryption Padding

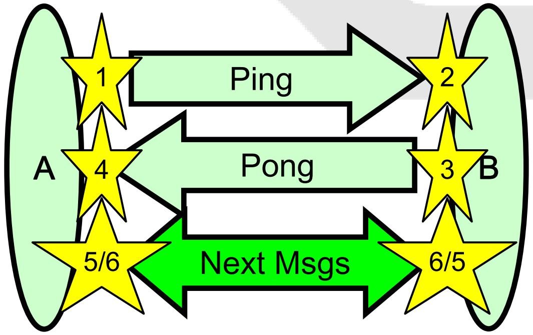
Secure, Type 1

May refer to the intended destination of the information

Should refer to the session keys and credentials agreed on between the sender and destination during an earlier ping pong

Encryption IV, Ping sender's certificate (only once, only if privacy issues

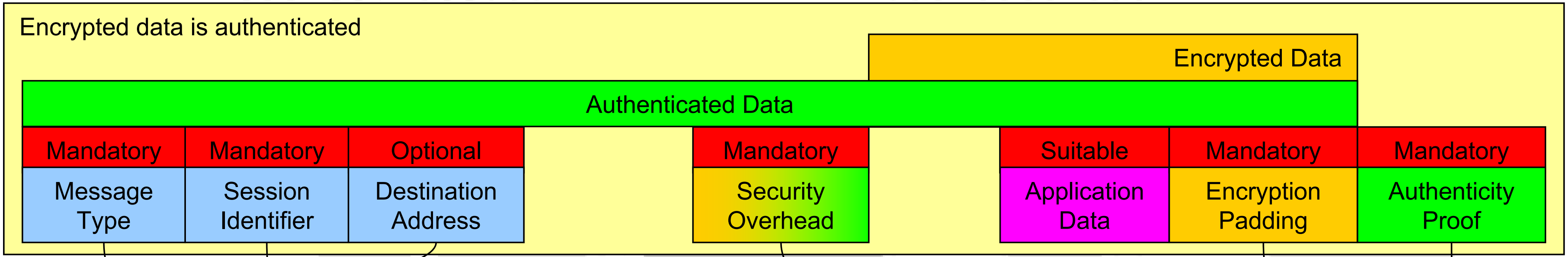
Makes the length of the plaintext data a multiple of the block cipher's block length



Note: A secure message must have been preceded by a ping pong

Application Related	Confidentiality Related	Authentication Related	Communication Session Related	Optionality

Message Details – Secure Message (Type 2)



Encrypted data is authenticated

Encrypted Data

Authenticated Data

Mandatory	Mandatory	Optional	Mandatory	Suitable	Mandatory	Mandatory
Message Type	Session Identifier	Destination Address	Security Overhead	Application Data	Encryption Padding	Authenticity Proof

Secure, Type 2

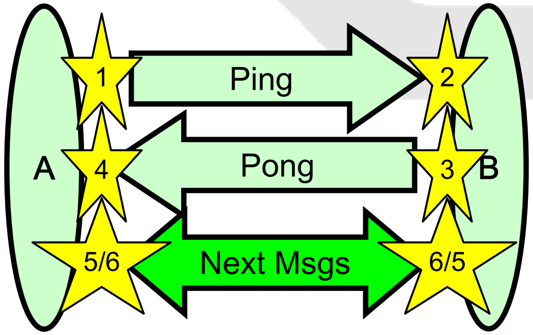
May refer to the intended destination of the information

Should refer to the session keys and credentials agreed between the sender and destination during an earlier ping pong

Encryption IV, Ping sender’s certificate (only once, only if privacy issues

Makes the length of the plaintext data a multiple of the block cipher’s block length

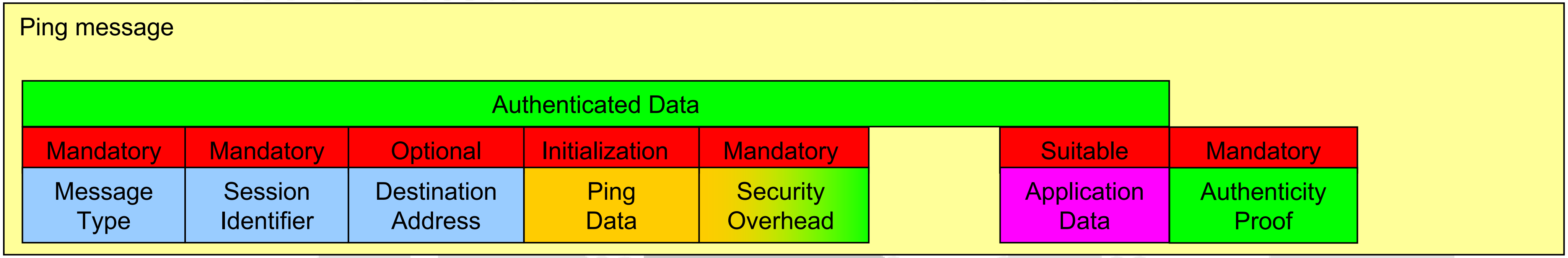
Digital signature or Message Authentication Code



Note: A secure message must have been preceded by a ping pong

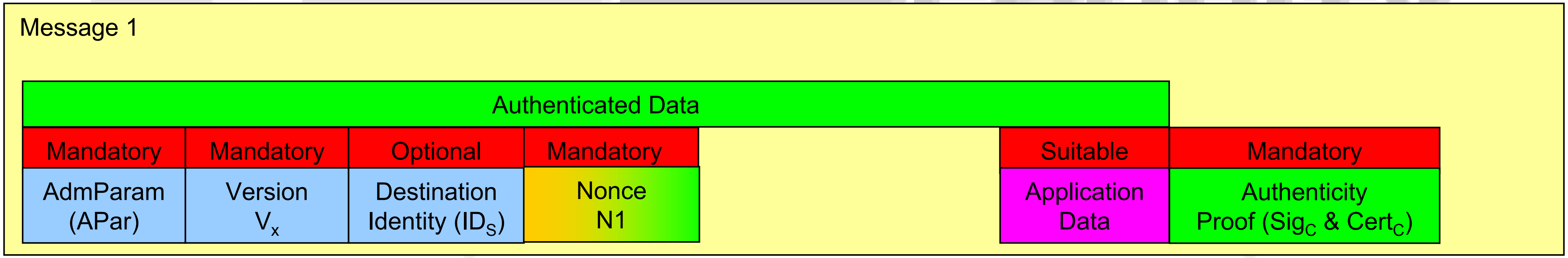
Application Related	Confidentiality Related	Authentication Related	Communication Session Related	Optionality

Message Details
Ping Message vs. Message 1



Ping message

Authenticated Data						
Mandatory	Mandatory	Optional	Initialization	Mandatory	Suitable	Mandatory
Message Type	Session Identifier	Destination Address	Ping Data	Security Overhead	Application Data	Authenticity Proof



Message 1

Authenticated Data					
Mandatory	Mandatory	Optional	Mandatory	Suitable	Mandatory
AdmParam (APar)	Version V_x	Destination Identity (ID_S)	Nonce N1	Application Data	Authenticity Proof (Sig_C & $Cert_C$)

- 🟪 Application Related
- 🟨 Confidentiality Related
- 🟩 Authentication Related
- 🟦 Communication Session Related
- 🟥 Optionality

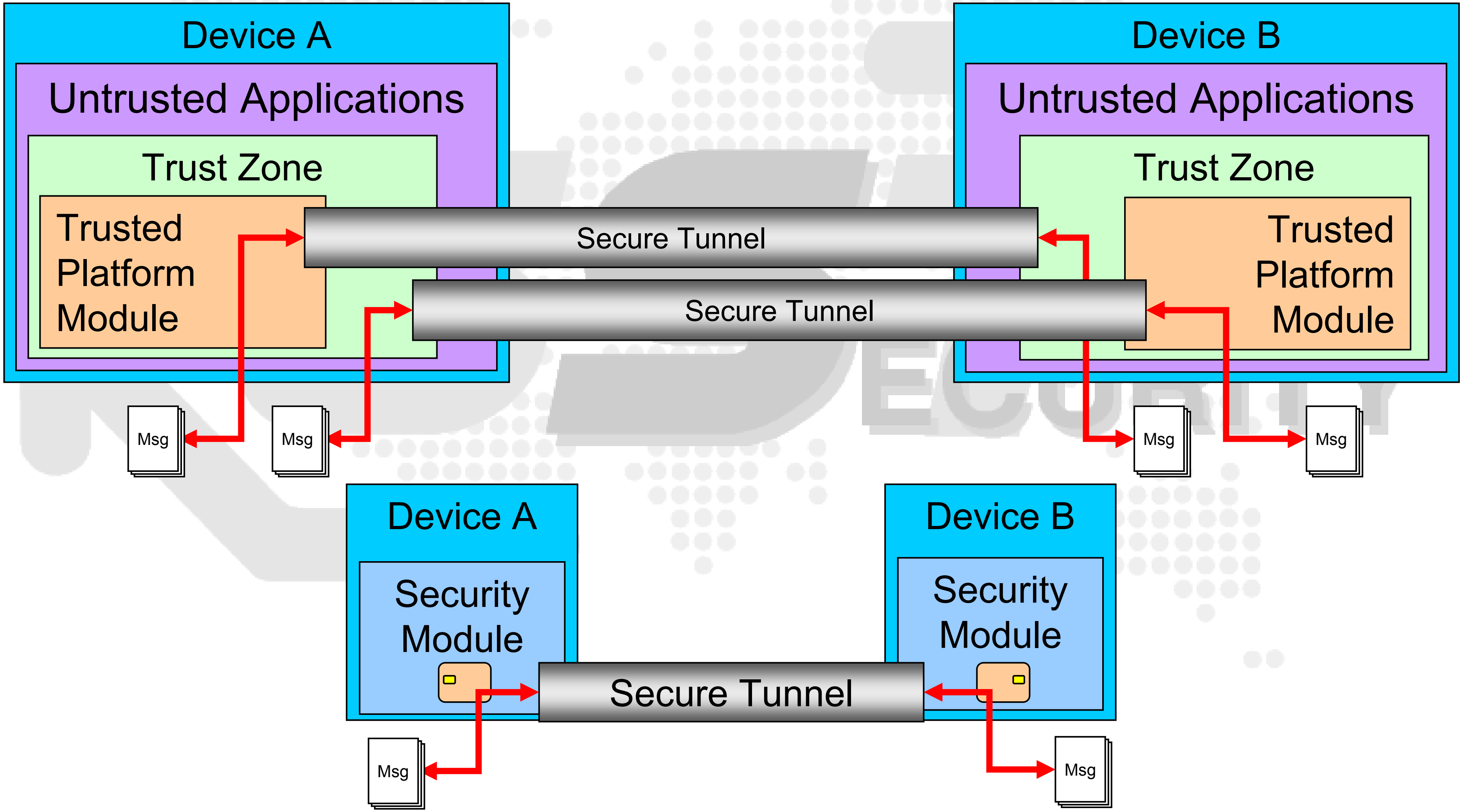
Examples of Security Modules

- Hardware security module (most expensive)
  - Used for high-bandwidth communications, secure payments, etc.
- Smartcard, SecurID token, SIM card
  - Commonly used to provide strong user, service and device authentication
- Trusted platform module (TPM)
  - By default built into many new laptops and desktops
  - Lacks features necessary for GST, e.g., authentication of users, application data, etc.
  - TPM only authenticates the device
- Software key store (cheapest)
  - Cryptography-related data is stored in persistent memory (flash, magnetic,…)
  - Non-secure microcontroller operates on this data

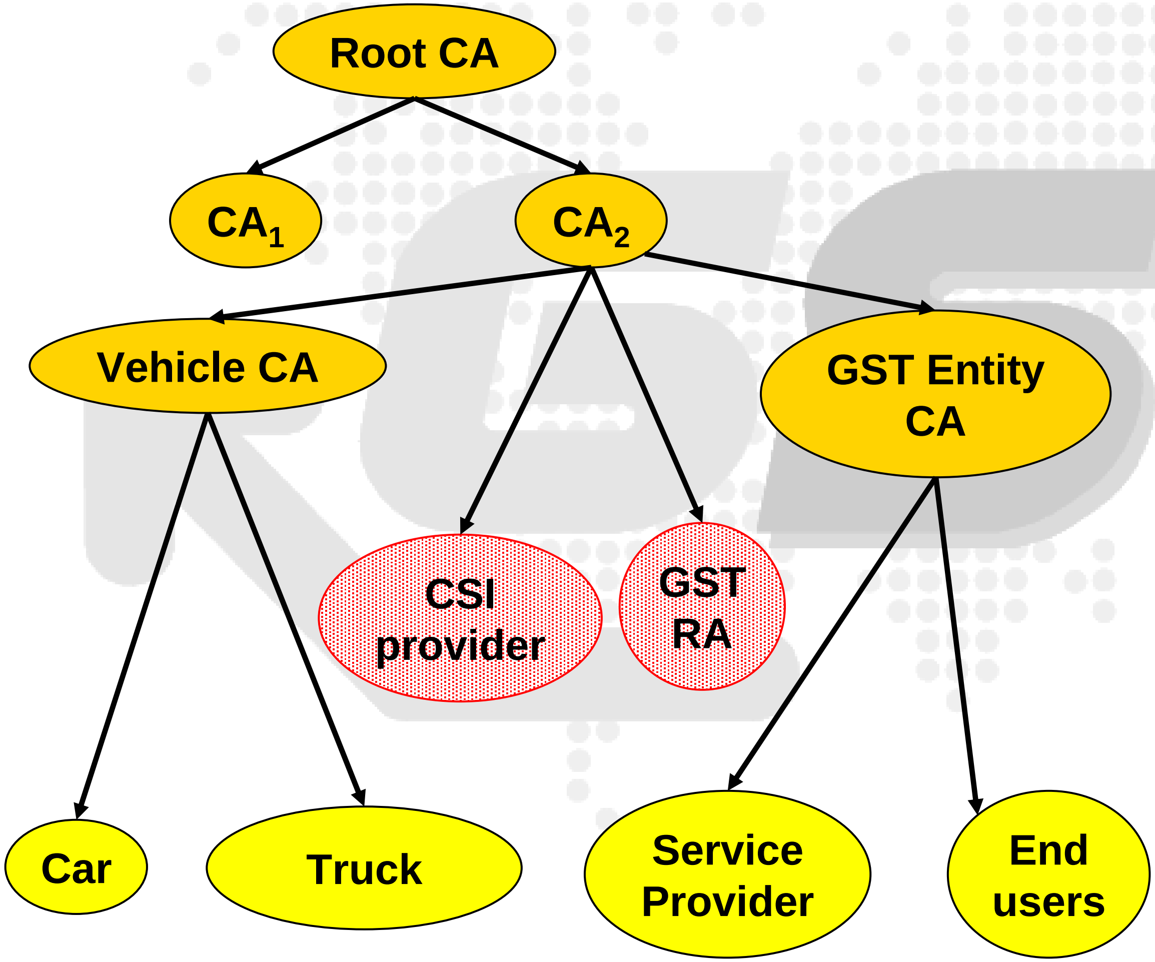
Different form factors:

- Dedicated coprocessor
  - Pluggable (e.g., reader for smartcard/memory card, SIM lock for SIM card, socket for chip
  - Fixed, e.g., soldered secure microprocessor (similar to smartcard, TPM)
- Using the main processor for functionality, coprocessor for important processes (e.g., payable services)
- Using the main processor only
  - Software-only security

Trusted Platform vs. Security Module



Example of Certificate hierarchy for GST involving a Root CA



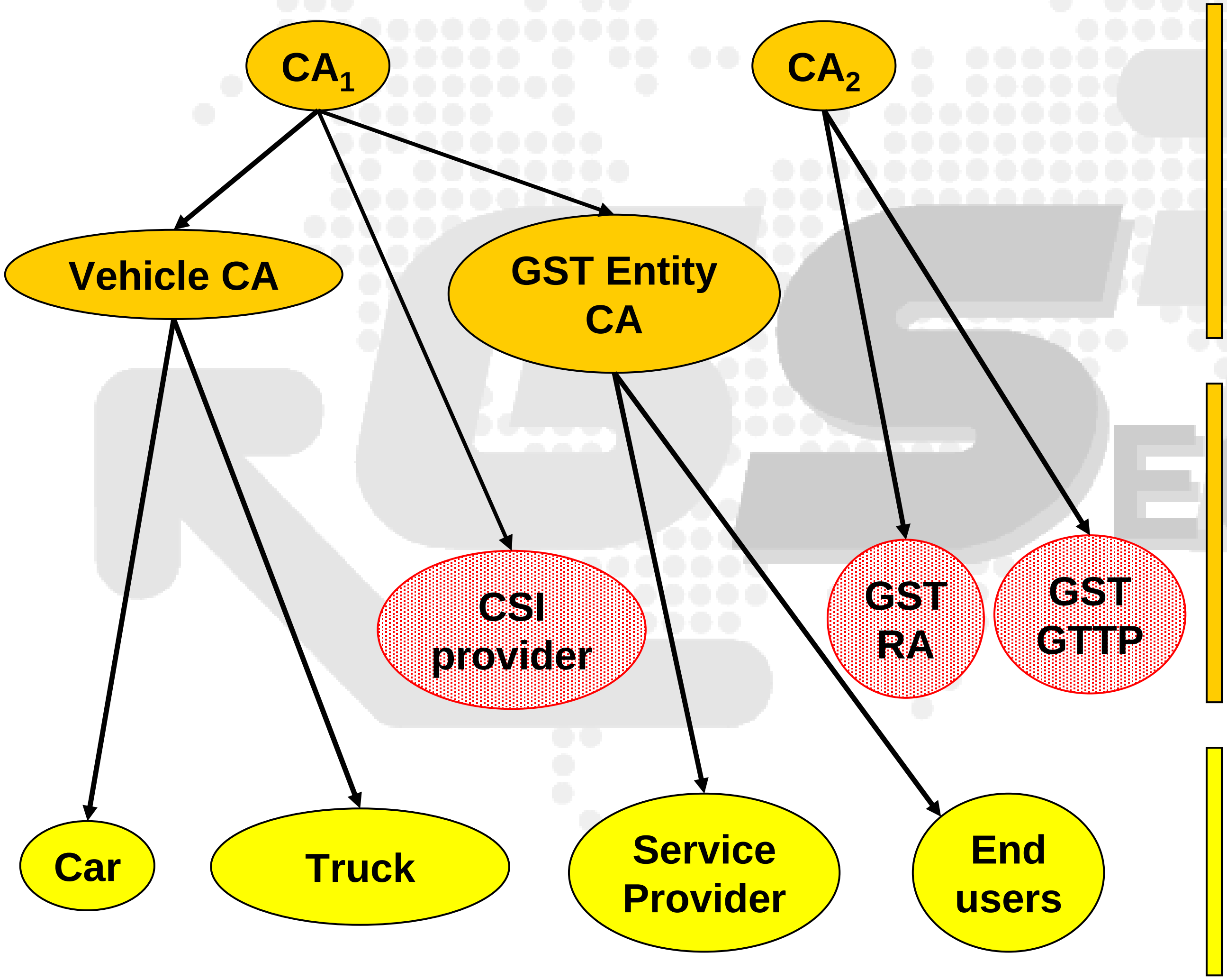
Root CA provides rules
Over Sub CAs

CAs issue
Sub CAs

RA and CSI provider
provide support services
related to Certificates

End point of
certificate chain

Example of Certificate hierarchy for GST without a Root CA



Sub CAs issue
Sub CA certificates

A Global Trusted Third Party (GTTP) issues a list of CAs which are trusted within GST

RA and CSI provider provide services related to Certificates

End point of
certificate chain