



A Security Architecture for Automotive Push and Pull Applications

Danny De Cock

Danny.DeCock@esat.kuleuven.ac.be
Katholieke Universiteit Leuven/Dept. Elektrotechniek (ESAT)
Computer Security and Industrial Cryptography (COSIC)
Kasteelpark Arenberg 10
B-3001 Heverlee
Belgium

These slides can be downloaded at <http://godot.be/slides>

- About GST
- Transversal nature of “security”
- Generic architecture
- Secure vs. Trust
- Security Modules

About GST



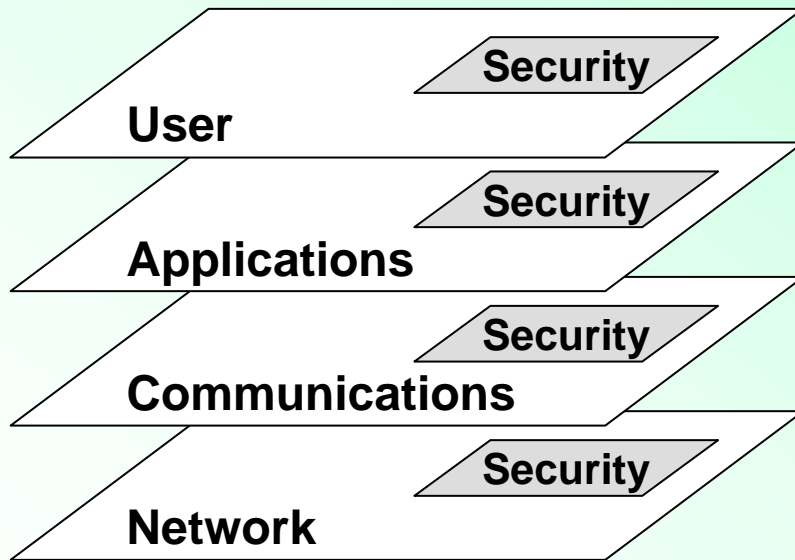
- Global System for Telematics (GST)
 - Integrated Project (IP) supported by the European Commission's Information Society Directorate General
 - Total budget: 21,5 million Euro with an EC contribution of 11 million Euro
 - Duration: March 2004 through February 2007 (36 months)
 - Contract N°: 507033, priority FP6-2002-IST-1

- Target:
 - Create an **open environment** in which innovative telematics services can be developed and delivered **cost-effectively**
 - Drivers and occupants have to be able to rely on their on-board integrated telematics system to **access a dynamic offer** of on-line safety, efficiency- and comfort-enhancing services wherever they drive in Europe
 - Drivers have to be able to **access their portfolio of services** throughout Europe using the same vehicle terminal

- 7 Subprojects:
 - Technology-oriented: Open Systems, Certification, Service Payment, Security
 - Service-oriented: Rescue, Enhanced Floating Car Data, Safety Channel

- Define an **architecture** and provide **security mechanisms** for secure telematics applications.
 - functional point of view (applications, services, user devices)
 - infrastructure point of view (networks, platforms)
- Define roadmap for a **trust value chain** including certification requirements

Security – Where?



**Strong authentication of
{user, device, service provider}**

Applications integrity

Secure communications

Network access

Focus

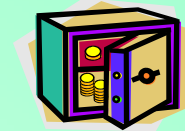




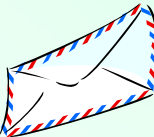

Security – How?



Based on implementation complexity and cost:

- No security mechanisms
- Non-cryptographic techniques (e.g., CRC, hardware enclosures,...)
- Combine all of the above with cryptographic techniques

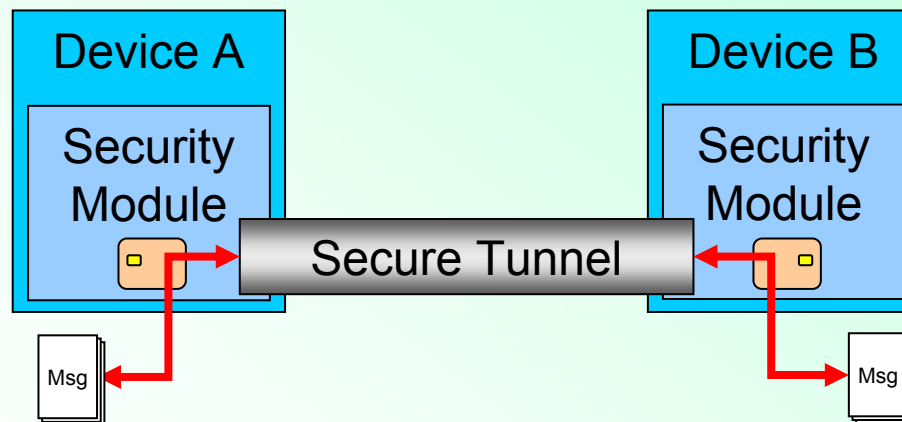


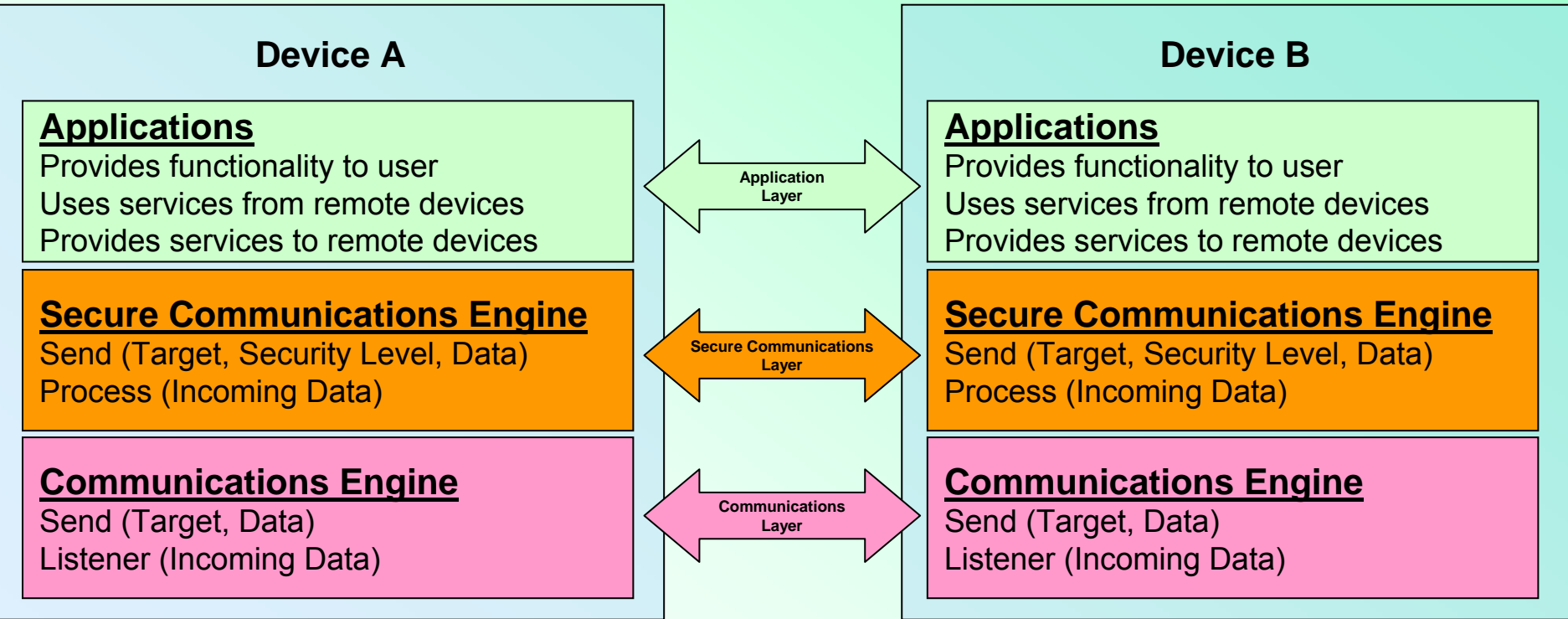
Security Levels		Protect Confidentiality	
		Yes	No
Protect Integrity	Yes	Secure 	Authenticated 
	No	Confidential 	Insecure 

Security – What?



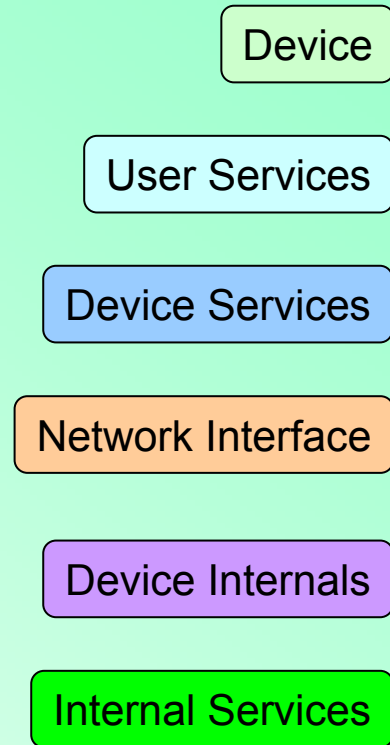
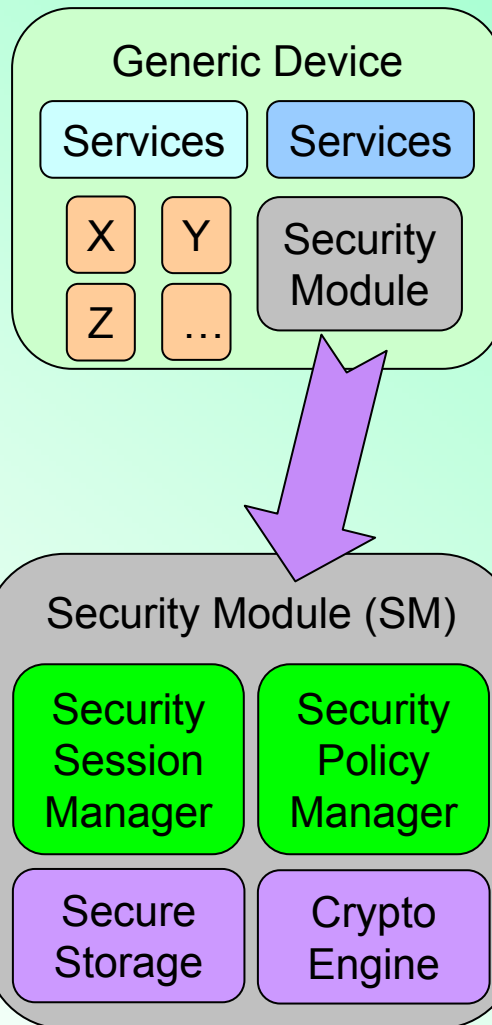
- User/Services data
 - User requests service
 - Information and data exchange
 - Service provider provides service
 - Client-server model
- Application data
 - Sent between service provider and device

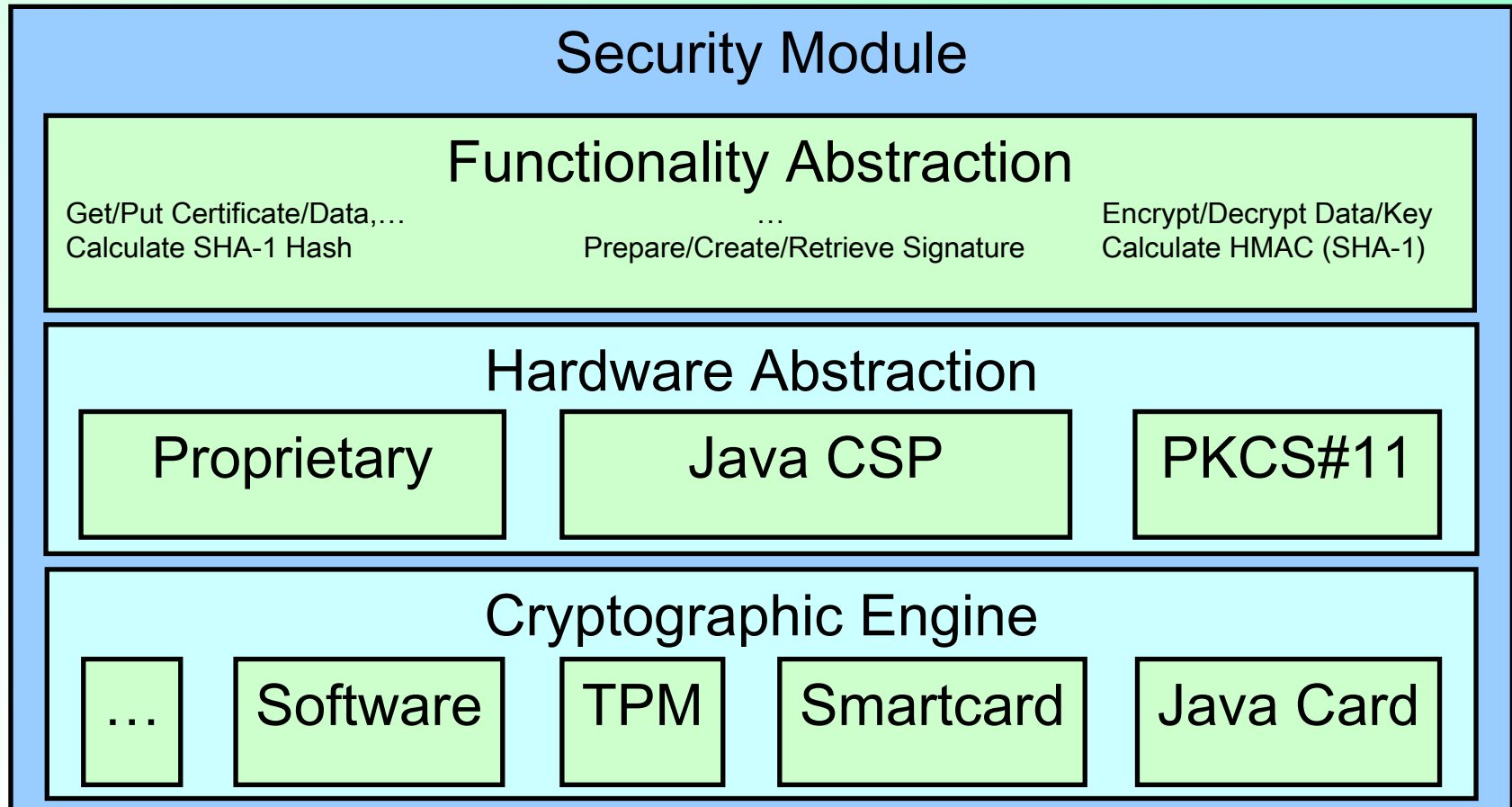




Key Features of a Security Module:

- One SM per Device
- SM = e.g., OSGi bundle
- SM offers services to other bundles
- SM initialized by manufacturer
- Initialized SM ready to be used
- Combination of hard- and software
 - Hardware → Non-cloneable
 - Software → Risk for cloning
- Provide true strong authentication
- Secure communications rely on SM
 - Insecure
 - Authenticity
 - Confidentiality
 - Secure = Auth. + Conf.

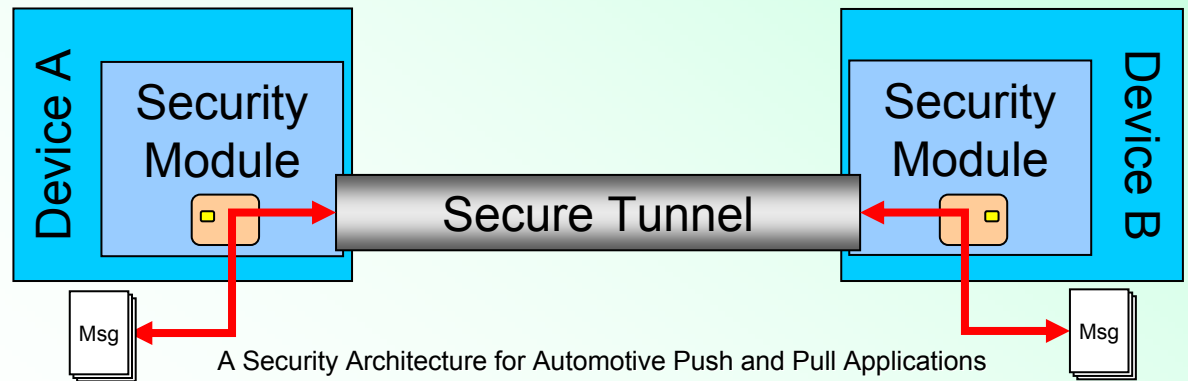
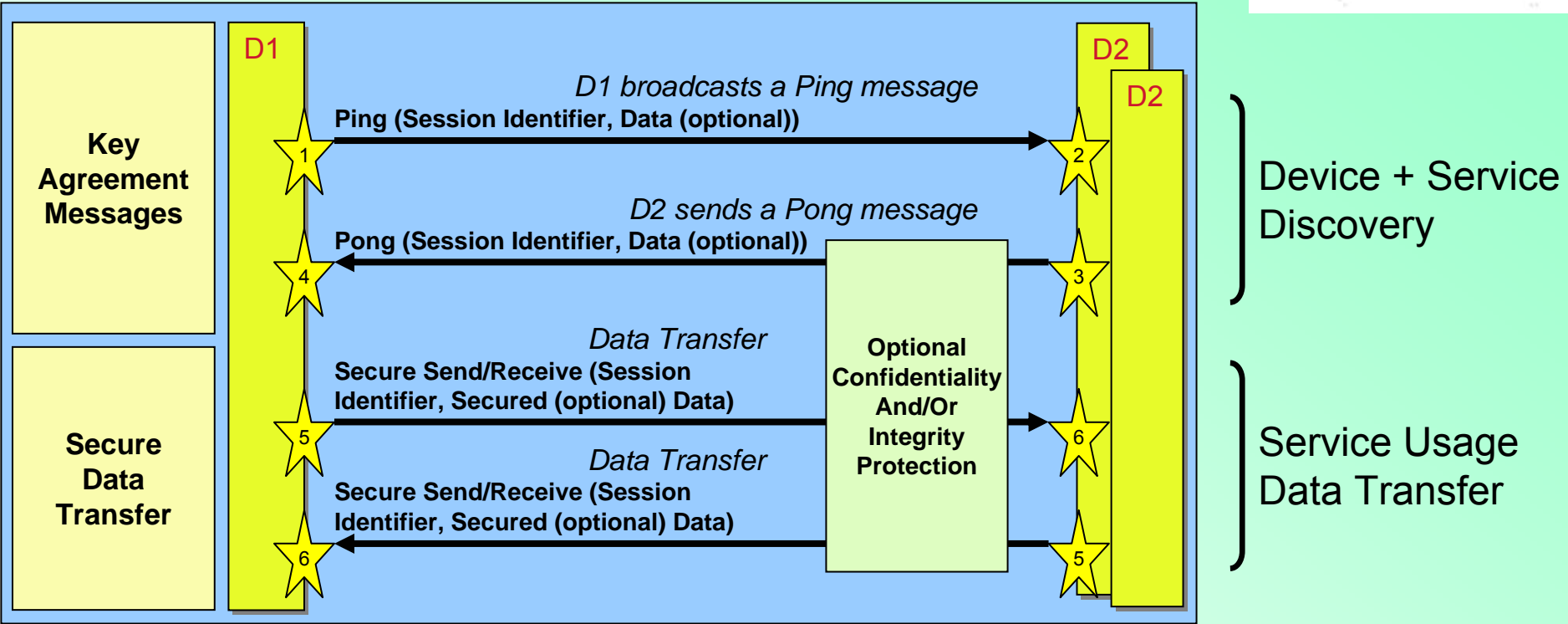




- Secure persistent storage engine
 - User data, Communications session data
- Authentication engine
 - Digitally sign outgoing information
 - Calculate Message Authentication Code
 - Verify incoming authenticated data
- System-wide “trusted” information
 - Root CA certificates
 - Trust anchors with respect to registration proofs

- Operates in client-server mode
 - Difficult to enforce use of security module at client side
 - Server can determine whether the correct SM was used

Secure Key Agreement with Station-to-Station



Secure Key Agreement with Station-to-Station (ctd)



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 $(data_1 || \alpha^x)$

D2 Receives a Ping message

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



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 $(E_K(data_2) || \alpha^y)$

D1 Receives a Pong message

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



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 $(E_K(data_3))$

D2 Receives a Secured Data Transfer message

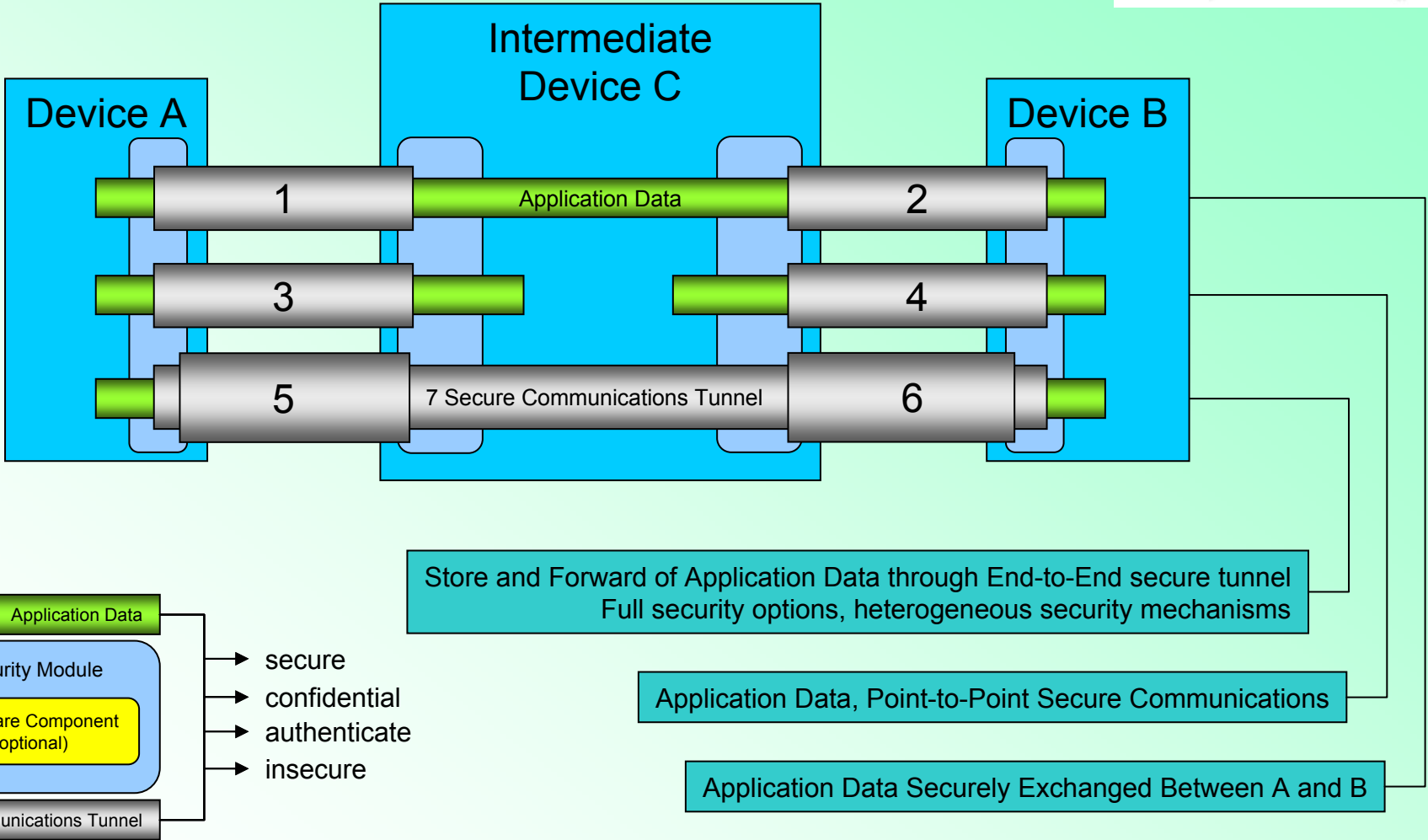
- Checks Authenticated $(E_K(data_3))$



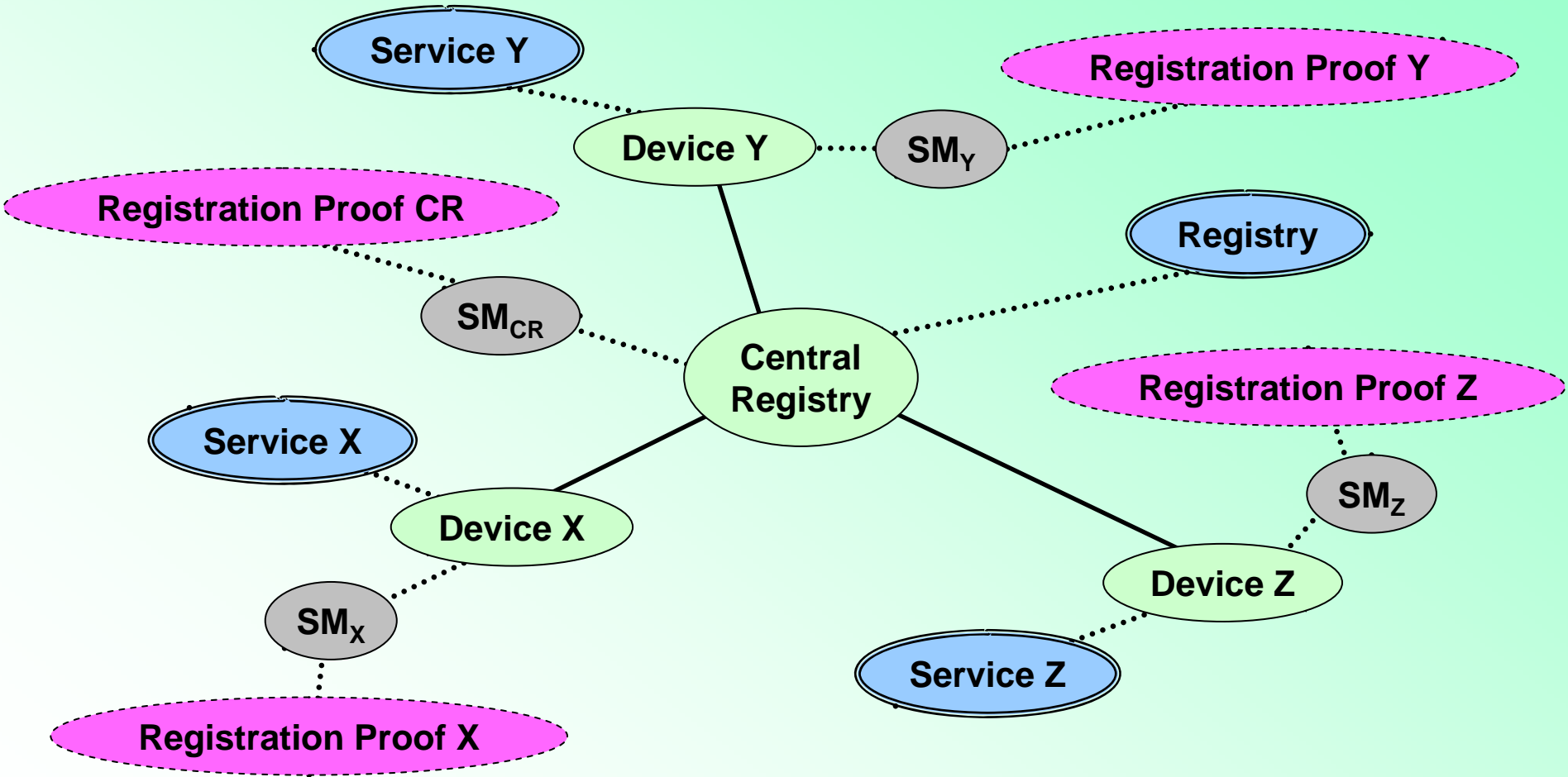
D2 Decrypts the information within a session with D1

- Decrypts $E_K(data_3)$

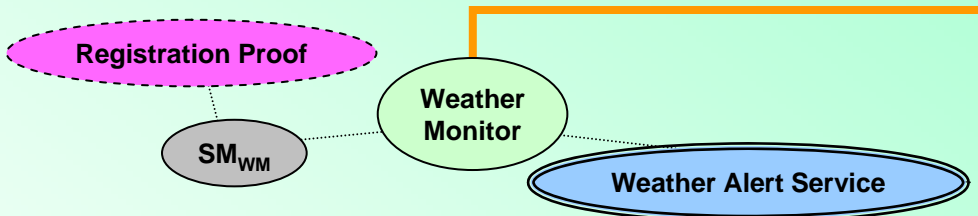
Secure Communication Types



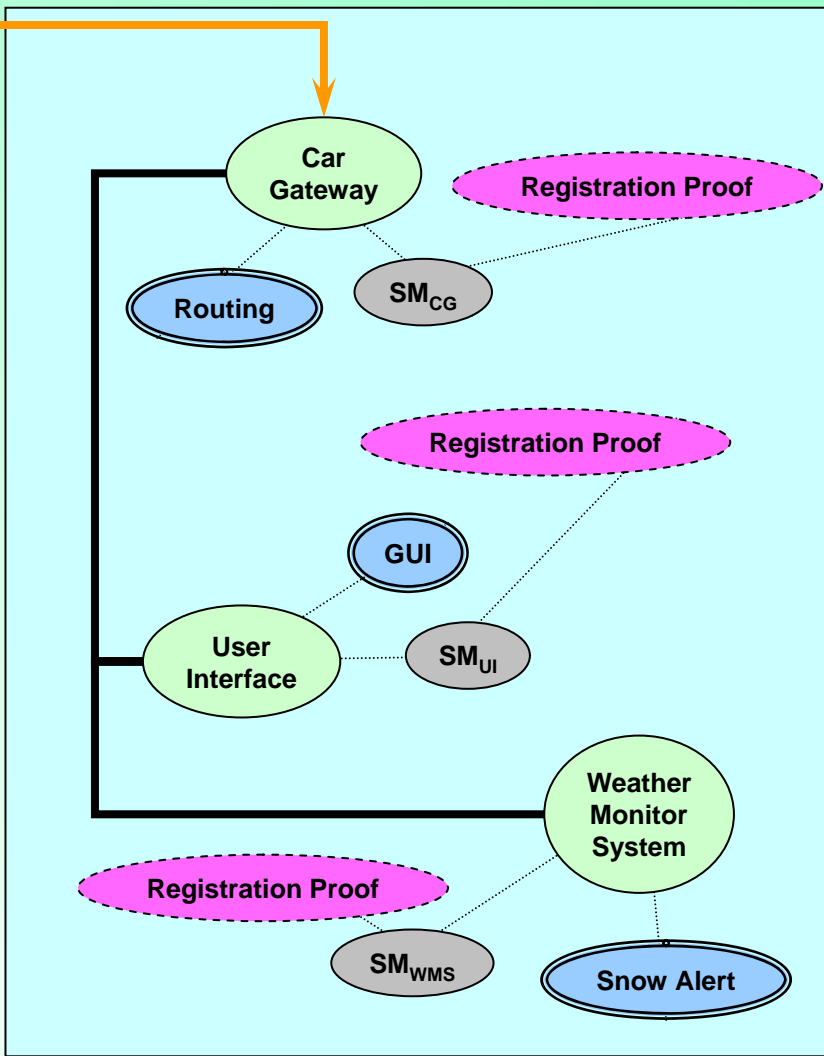
Devices Registration



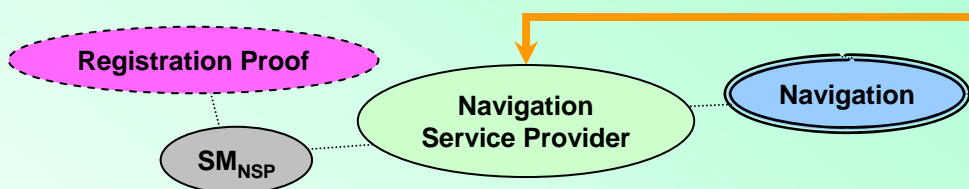
Pushing Data to Car



- Information is sent to a vehicle
- Vehicle gateway determines information origin
- If “trusted”, information routed to intended destination
- Registration proofs are crucial to build trust
 - Determine whether a device in a car belongs to that car

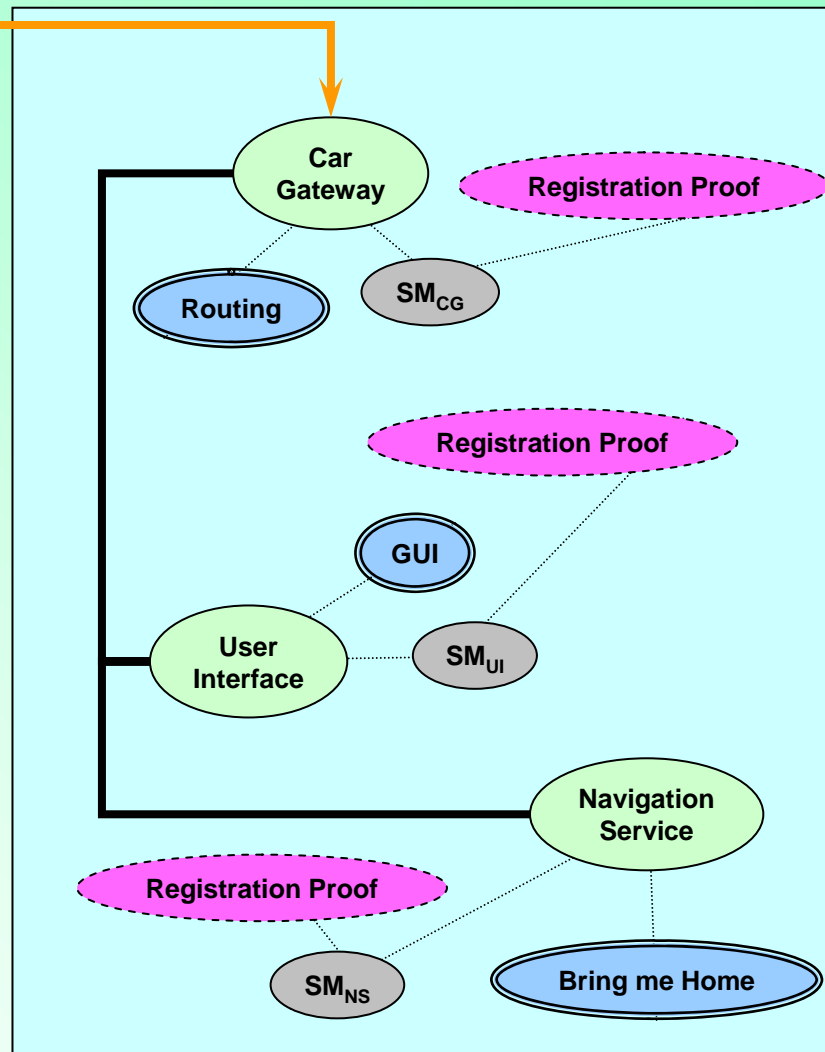


Pulling Data to Car



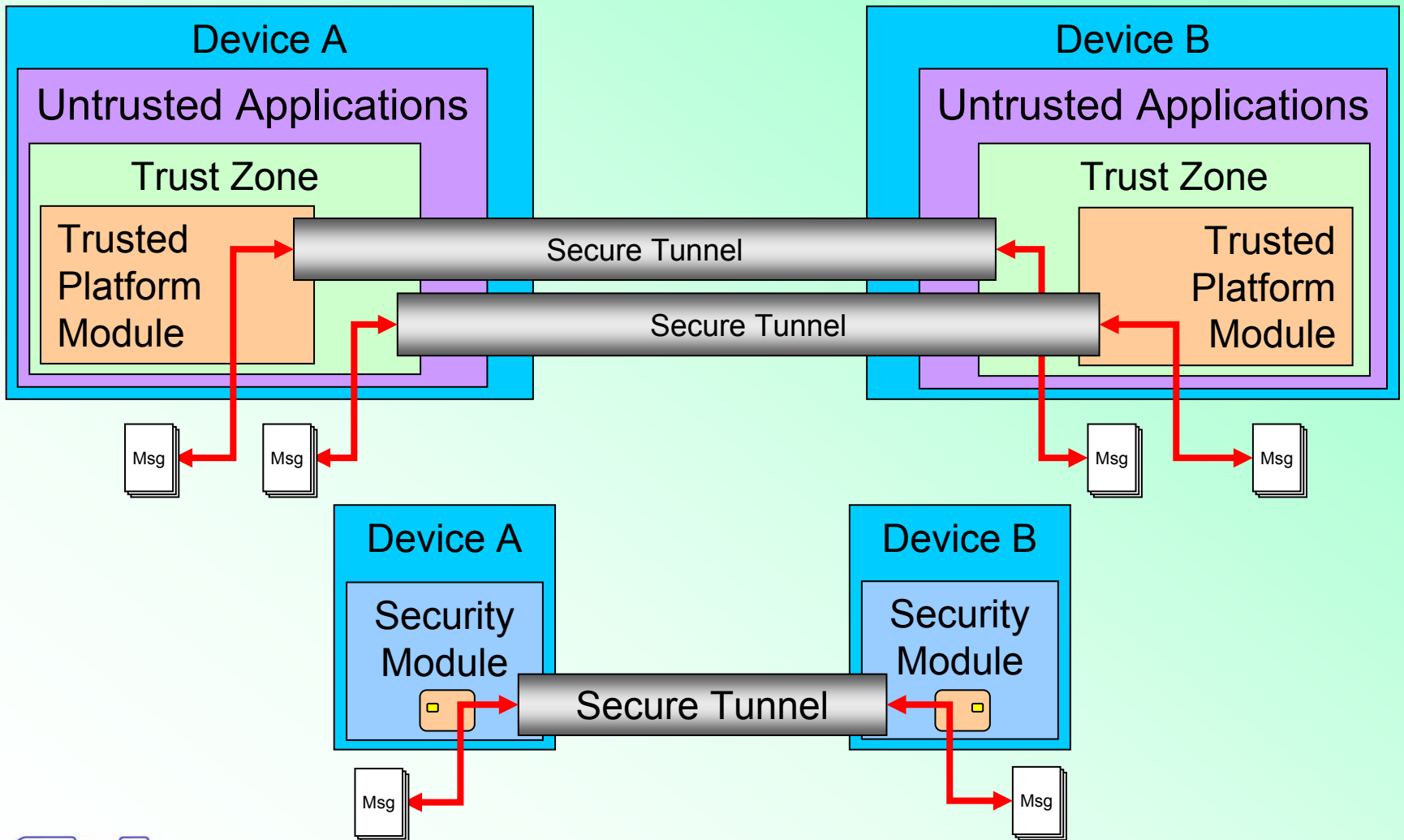
- In-car service requests Car Gateway to send a request to a remote Service Provider
- Service Provider determines request origin
- Authorized request is processed
- Response is authenticated and sent to requestor if applicable

- Allows proving who used a specific service, e.g., for billing



- Hardware security module (most expensive)
 - Used for high-bandwidth communications, secure payments, etc.
 - Not very car-friendly 😊
- Smartcard, SecurID token, SIM card
 - Commonly used to provide strong authentication
 - Reasonably cheap
- Trusted platform module (TPM)
 - By default built into many new laptops and desktops
 - Cheap
- Software key store (cheapest)
 - Less critical applications

Relation with Trusted Computing



Conclusions



- Need for strong user and device authentication
- Registration proofs provide security context
- Security modules are more than a TPM

Thank you for your attention

Danny De Cock

Danny.DeCock@esat.kuleuven.be

<http://www.esat.kuleuven.be/cosic>

GST – Global System for Telematics

<http://www.gstforum.org>

“If it is provably secure, it is probably not...” – Lars R. Knudsen on block ciphers

Protocol Stacks View

