RPC Encryption

SDLC Project Maintainer

Target Goal

Prevent unauthorized viewing of RPC communication between an SDL-enabled app and SDL Core through data encryption.

Solutions Considered

- Use policy table to flag individual RPCs to encrypt
  - New “RPC Management” section in Policy Server
  - Developers required to check each RPC’s security
- Use policy table to flag transport as encrypted (“All or Nothing”)
  - Encryption handshake attempted immediately after app connects to Core
  - If handshake is successful, all RPCs are encrypted

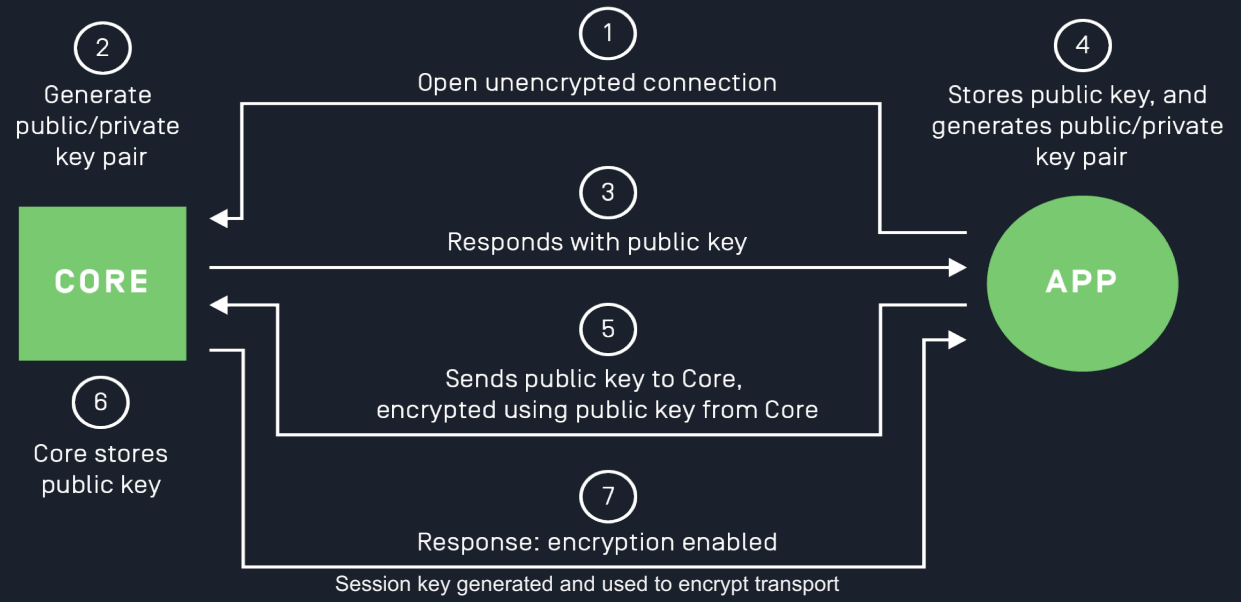
Comparison

	Individual RPC Protection	Transport level Encryption
Could encrypt all existing RPCs*	YES	YES
Encrypts future RPCs without OEM action	NO	YES
Limits security fragmentation across OEMs	NO	YES
Minimizes changes and complexity of Policy Server	NO	YES
Simplifies app developer integration	NO	YES

Why “All or Nothing”

- The web as a whole is moving towards encrypting everything
- SDL cloud apps are requiring secure transports (WSS)
- App developers will perform fewer checks to see if each RPC they will use is secure, they can check if their transport is secure (1 vs. n)
- We should not be deciding whether an app developer uses an RPC in a manner that should be protected or not (ex. A Show RPC with protected information).
- As vehicles become more connected, RPC level encryption would create technical debt that would be extremely difficult or impossible to remove long term

“All or Nothing” Flow Diagram



*Pseudo-Flow for transport encryption without adding ‘security libraries’