

# SMART CHARGING AND VEHICLE-TO-GRID (V2G) SUPPORT ON S32G2 PROCESSORS

## S32G2 Safe and Secure Vehicle Network Processors

### OVERVIEW

Smart charging enables a bidirectional charging infrastructure consisting of electric vehicles, charging stations and charging operators. Data communications between the interfaces are on a secure channel. ISO 15118, the standard for communication between electric vehicles (EVs) and charging stations, allows for a user-friendly “plug and charge” mechanism for authentication, authorization, billing and flexible load control based on information exchanged between an EV and the charging infrastructure.

Some characteristics of smart charging include:

- No credit card or payment method requirement for charging a vehicle; the EV identifies itself to the charging station and gets the authorized access to the energy for charging its battery
- Energy transfers from the EV to the charging station and vice versa; this helps prevent overloading of the electric grid
- Wireless or wired software updates can occur during charging

### S32G2 HARDWARE SECURITY ENGINE FEATURES

- The hardware security engine (HSE) is a security subsystem that runs relevant security functions for confidentiality, data integrity and authenticity
- HSE security engine firmware operates on a dedicated Arm® Cortex®-M7 core running at 400 MHz and utilizing its own secure RAM and ROM

The HSE subsystem features the following cryptographic accelerators:

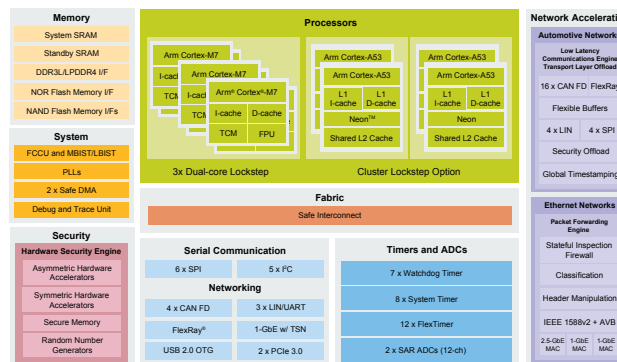
- A TDES engine
- An AES engine supporting all standard key sizes (128, 192, 256 bits) and various complex ciphering modes (CBC, CTR, GCM, etc.)

- A hash engine supporting standard SHA1 and SHA2 hash primitives up to 512-bit digest
- A public key cryptographic (PKC) engine which accelerates RSA and ECC operations
- Supported symmetric and asymmetric cryptography

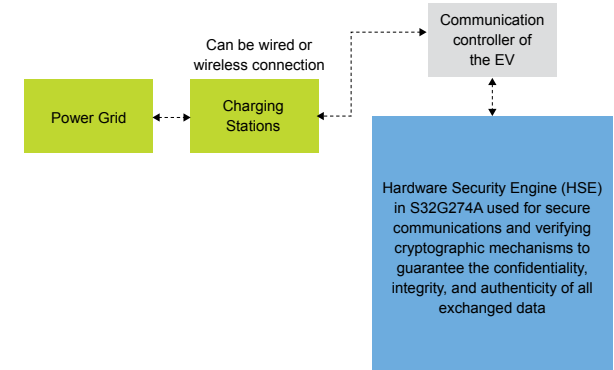
### ENABLEMENT TOOLS

- S32 Design Studio for S32 platform processors with configuration tools
- S32 debugger probe enables debugging and trace for S32G2
- Real Time Drivers combining functionalities of SDK and MCAL as single software product for single S32 families
- Linux BSP the reference software for Arm Cortex-A53 cores
- HSE firmware enables hardware security module integrated with S32G2
- FreeRTOS the real-time OS for Arm Cortex-M7 cores

### S32G2 BLOCK DIAGRAM (S32G274A)



### SYSTEM BLOCK DIAGRAM



### ISO 15118 AND RELATION TO OSI LAYERS

Application OSI Layer	ISO 15118-1	ISO 15118-2	ISO 15118-3	ISO 15118-5	ISO 15118-8	ISO 15118-9
Application OSI Layer 7		Application layer messages (V2G message), SDP (SECC Discovery Protocol)				
Application OSI Layer 6	Network and application protocol requirements	EXI (Efficient XML Interchange)				
Application OSI Layer 5	General information and use case definition	V2GTP (Vehicle-to-grid Transfer Protocol)				
Application OSI Layer 4	2nd generation network and application protocol requirements	UPD (User Datagram Protocol), TCP (Transmission Control Protocol), TLS (Transport Layer Security)				
Application OSI Layer 3	(merged with contents of ISO 15118-6 for second edition)	IP (Internet Protocol), SLAAC, DHCP				
Application OSI Layer 2	Physical and data link layer requirements	Physical and data link layer conform. tests	Physical and data link layer requirements for wireless communication			
Application OSI Layer 1			Physical and data link layer requirements for wireless communication			Physical and data link layer conformance test for wireless comm.