



## Factsheet 03: Secure Channel Protocols

As technology continues to evolve, so does the need for secure communication between devices. Embedded devices such as microcontrollers, sensors, and secure elements frequently exchange sensitive information, making them attractive targets for cyberattacks. Secure Channel Protocols (SCP) play a vital role in safeguarding these exchanges, ensuring that data remains private and secure.

The **ORSHIN project** focuses on developing resilient hardware and software for the Internet of Things (IoT). This research aims to improve the security of intra-device communications – ensuring that information flowing within a device is protected from unauthorized access.



### Why Are Secure Channel Protocols Important?

Modern devices must ensure that communication is secure, particularly when sensitive data such as cryptographic keys, personal information, or proprietary data is involved. Secure Channel Protocols guarantee:

- **Confidentiality:** Prevents unauthorized users from reading the data.
- **Integrity:** Ensures that data is not altered during transmission.
- **Authentication:** Verifies the identity of the devices communicating.

Securing these communications is especially challenging for embedded devices, which often have limited processing power and memory. Therefore, it is crucial to use secure yet efficient protocols.

### Phases of Secure Communication

Secure communication protocols typically follow three key phases:

1. **Provisioning:** In this phase, cryptographic keys and other necessary security parameters are installed on the device. This allows the device to set up secure communication channels with other trusted components.
2. **Handshake:** The components involved in the communication establish a secure connection by exchanging cryptographic information. This phase ensures that both components agree on how to communicate securely.
3. **Data Exchange:** Once the secure connection is established, data can be transmitted between the components. This phase is protected by encryption and verification mechanisms, ensuring that the data remains secure and authentic throughout the process.

### Emerging Trends and Challenges

Emerging trends in secure communication protocols focus on enhancing security and performance, with lightweight cryptography gaining attention for improving efficiency in resource-constrained devices. While Secure Channel Protocols (SCP03) and Replay Protected Memory Block (RPMB) use traditional cryptographic methods, lightweight alternatives can offer better performances. Sponge cryptography, used in frameworks like Noise and Blinker, improves security by continuously updating the cryptographic state and verifying message integrity.

### Key Insights from the Research

The **ORSHIN project** has highlighted several key findings regarding the state of secure channel protocols:

- **Protocol Phases:** Secure communication protocols generally follow three stages: Provisioning, Handshake, and Data Exchange, each of which has specific security requirements.
- **Standard vs. Proprietary Protocols:** While standard protocols like SCP03 and RPMB offer broad applicability, many manufacturers create their own proprietary solutions to meet specific product needs. These proprietary protocols can offer performance optimizations but may require careful scrutiny to ensure they meet security standards.
- **Emerging Security Needs:** New techniques, such as lightweight cryptography and sponge cryptography, are likely to shape the future of secure communication, particularly for IoT and embedded devices.

### Conclusion and Future Directions

As embedded devices become more ubiquitous, the need for secure and efficient communication continues to grow. The research conducted by ORSHIN has provided a comprehensive analysis of both standard and proprietary secure channel protocols, highlighting the strengths and weaknesses of each.

Looking forward, **lightweight cryptography** and **sponge-based methods** offer promising avenues for improving the performance and security of secure communication protocols. These innovations could provide faster, more efficient ways to secure intra-device communications while maintaining robust protection against attacks.

Researchers and manufacturers alike should explore these evolving techniques to stay ahead of security threats and ensure that embedded devices can communicate securely in the increasingly connected world.

#### Glossary

- **Secure Channel Protocol (SCP):** A set of standards for securing data exchanges between devices.
- **Lightweight Cryptography:** Cryptographic algorithms optimized for devices with limited resources.
- **Sponge Cryptography:** A cryptographic method that continuously updates the shared cryptographic state during communication.