Cryptography & Authentication in IoT

Securing Devices, Data, and Communications

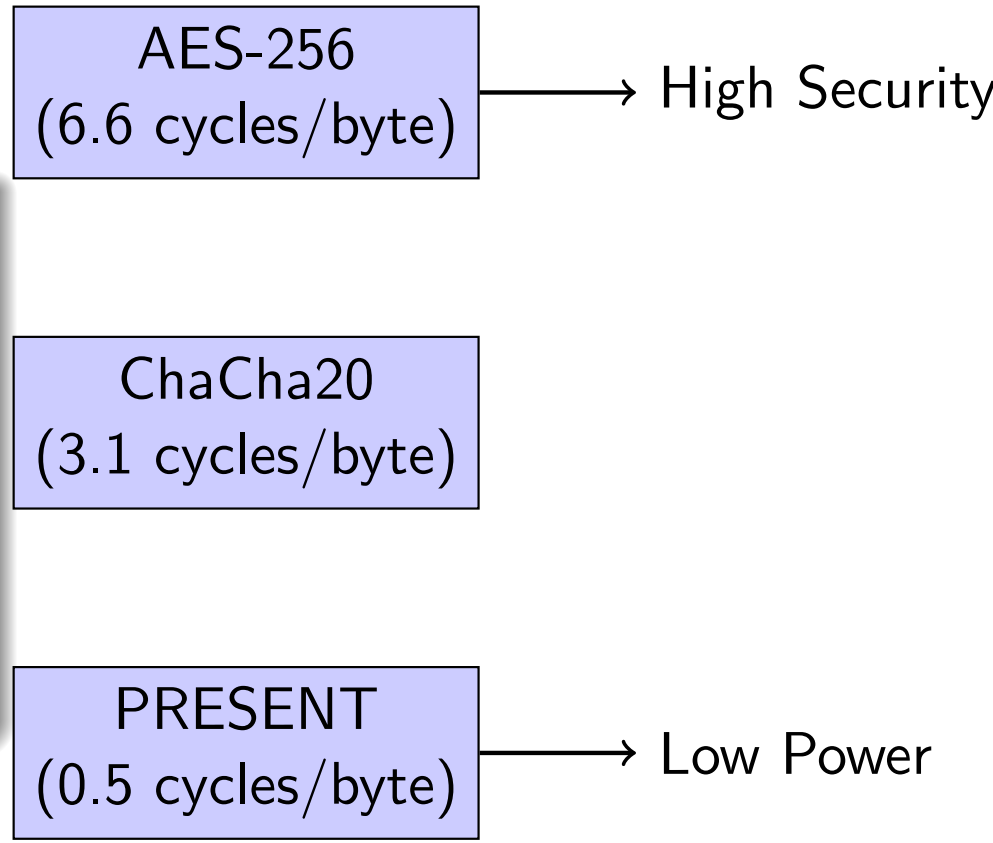
Dr. Öğr. Üyesi Yıldıran YILMAZ

Recep Tayyip Erdoğan Üniversitesi

Lightweight Cryptographic Algorithms

Key Algorithms

- **AES-128/256**: Gold standard for symmetric encryption
- **ChaCha20**: Faster than AES on low-power devices
- **PRESENT**: Ultra-lightweight block cipher



Protocol Security Comparison

Secure:

TLS 1.3
Full encryption
Perfect Forward Secrecy

For UDP:

DTLS
UDP variant of TLS
Handshake fragmentation

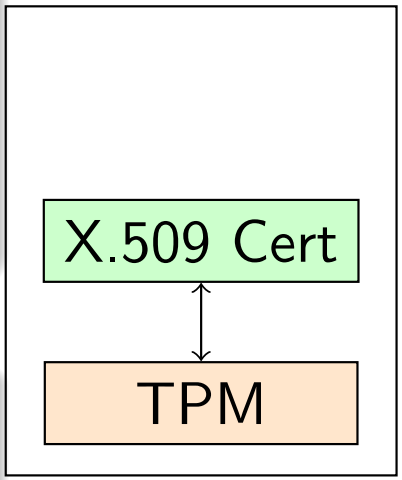
For MQTT:

MQTT-SN
Topic name encryption
QoS security

X.509 Certificates & TPM

Implementation

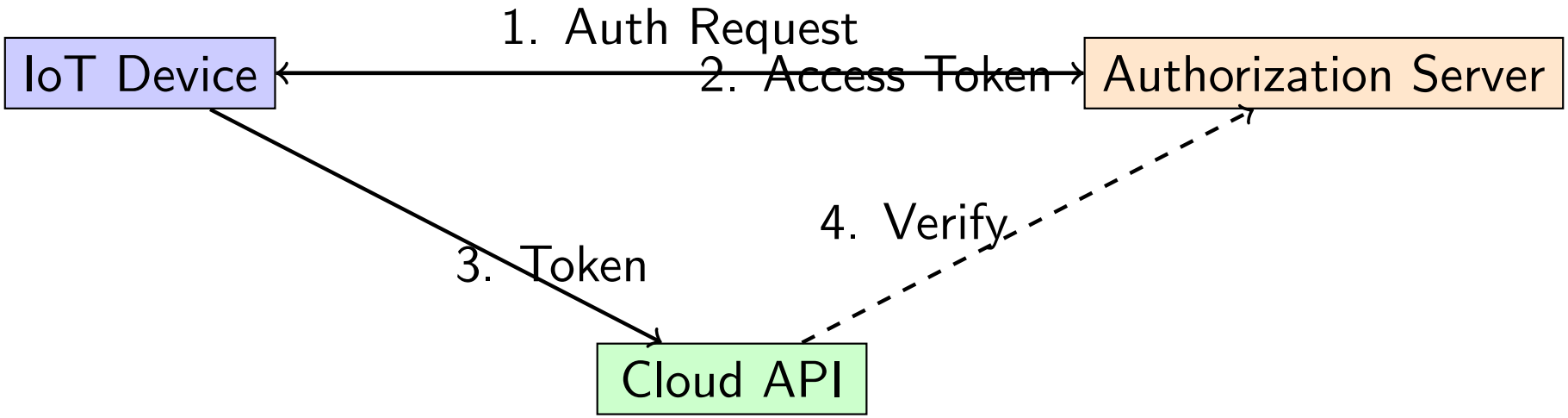
- **X.509**: Standard for PKI in IoT
- **TPM 2.0**: Hardware-based key storage
- **Secure Element**: Dedicated crypto chip



Challenges

- Certificate revocation in large deployments
- TPM cost vs. security trade-off

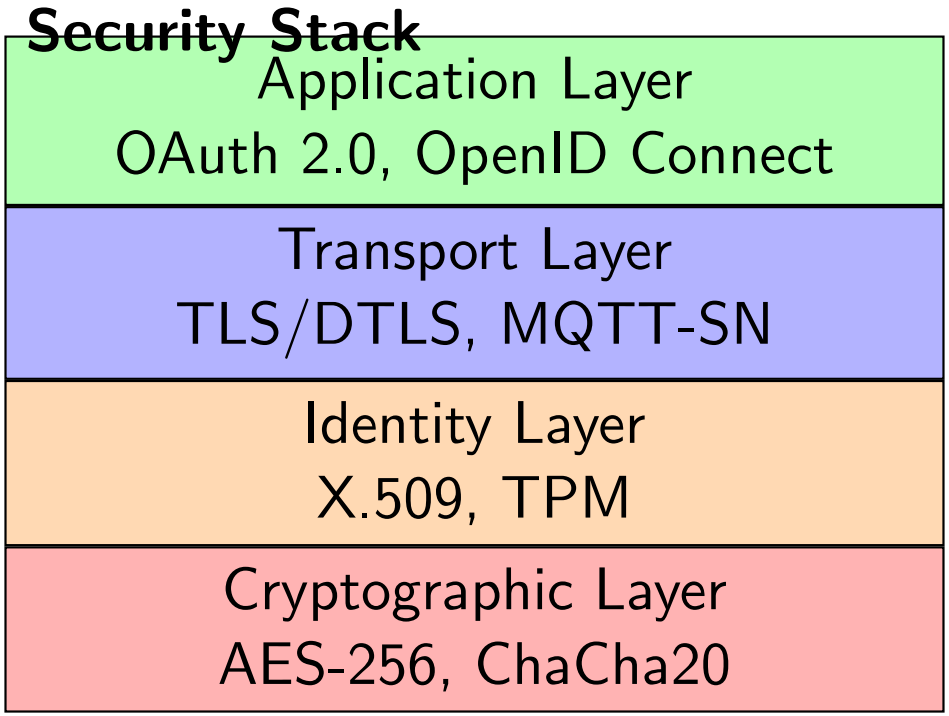
OAuth 2.0 & OpenID Connect



IoT-Specific Considerations

- Device Flow for headless devices
- JWT instead of cookies
- Short-lived tokens

Complete Security Stack for IoT



Key Takeaways

Cryptography

- AES for high-security
- ChaCha20 for efficiency

Identity

- X.509 for device identity
- TPM for key protection

Protocols

- Always use TLS/DTLS
- Prefer MQTT-SN over plain MQTT

APIs

- OAuth 2.0 for authorization
- OpenID Connect for authentication

Thank You!

Email: y.yilmaz@erdogan.edu.tr