Expert Community

Atos Breakout session
11 09 2019 – 10.30

TLS evolution
TLS evolution: from TLS 1.2 to PostQuantum ciphers”

Philippe Bodden & Slim Bettaieb
& Loïc Bidoux

Trusted partner for your **Digital Journey**

Atos

TLS evolution

"TLS evolution: from TLS 1.2 to PostQuantum ciphers"

Expert Community

Abstract

SSL/TLS is a major component of **security controls** that support most information systems designed and managed by Atos and Worldline.

It is paramount to position it adequately in the **security architecture** and to keep it **up to date** in a timely and systematic way, particularly when facing Internet.

Compliance with industry standards and regulatory requirements can be measured through **standard grades** that are widely accepted.

Purpose of the presentation is to:

- remind how TLS is articulating **underlying ciphers**
- propose how and where to position TLS to optimize the **security architecture**
- explain the current target **TLS 1.2 or 1.3**, and how to reach it with the appropriate ciphers
- list various categories of **threats**

Atos

TLS evolution

"TLS evolution: from TLS 1.2 to PostQuantum ciphers"

Expert Community

Abstract

- Among long-term future menaces, « Quantum Computing » is certainly one of the most far-reaching, as it will negate the security level provided by current asymmetric ciphers as we know them.
  - This means that « **Post-Quantum ciphers** » must be available on classic computers before attackers can gain access to the first Quantum computers.
  - As for TLS, this would mean getting some **one-to-one replacement** for asymmetric ciphers as used in key exchange and certificate authentication.
  - As a strong leader in Quantum technologies sensu lato, we are also already actively investiging Post-Quantum ciphers, including with TLS.
- The presentation will show that:
  - We have a clear short- and long-term strategy for securing data in transit,
  - Both customer and Atos perspectives are covered in a realistic way in terms of complexity, costs and digital transformation.

Atos

TLS evolution

"TLS evolution: from TLS 1.2 to PostQuantum ciphers"

Expert Community

Presenters:

Philippe Bodden

Enterprise & Security Architect (CISSP, CCSP, SABSA, TOGAF, COBIT):

Security

- Senior Atos Expert in Cybersecurity
- Security architecture & risk analysis
- Special interest in crypto, digital signature, quantum technologies

Slim Bettaieb

Slim has a PhD in computer science, and his thesis was about the design of new privacy friendly signature schemes based on lattices. He is working for the Worldline R&D team since 2014 as a security expert, on applying cryptography to online services and authentication protocols for payment

Loïc Bidoux

Loïc Bidoux has completed both an engineer degree and a PhD in computer science. He is working for the Worldline R&D team on applying cryptography to online services. His areas of interest notably include quantum-resistant cryptography and privacy.

Atos