

Accelerating the PQC transition of Operational Technology (OT)

Siemens AG, Dr. Alexander Railean

Multiple hybrid certificate formats grew at IETF, additional guidance is needed

- From 6 drafts → 3 are still around
 - Alive: Related-cert (RFC 9763), Composites, cert-discovery
 - Stopped: Chameleon, Sun Huawei, Truskovsky (lives on in ITU-T and X9.146)

How to help:

- Provide feedback about the whitepaper
- Share your success stories and failures
- Cross-industry collaboration

What we did about it internally

- Whitepaper describing each approach and comparing them in different scenarios
 - Guiding questions to assist in choosing
 - Draft of a decision-tree to start a conversation
- Individual IETF draft[†] about [migration use-cases](#)

OT use-cases are under-represented at IETF, collaboration can be improved

- The IETF is focused on use-cases for the public Internet and cloud providers.
- OT-related requirements are not a priority.
- IETF protocols are an inherent part of OT standards and existing deployments.

- Duplication of effort in various OT standards.
- The PQC transition is slower.

Specifics of the OT environment:

- Very long-living assertions, e.g., for trust anchors, IDevID certificates, fw/sw signatures
- Availability matters more than integrity or confidentiality
- Network isolation, limited or no Internet connectivity
- Hash-then-sign mode required

Examples of friction points:

- TLS 1.3 integrity-only, RFC 9150 → independent draft, not adopted by TLS-WG, therefore not widely known; but used in power systems: IEC 62351-3
- KEM-TLS not adopted by TLS-WG
- ECU for Configuration, Updates, and Safety-Critical Communication, RFC 9809 → heavy push-back from LAMPS-WG due to OT focus

Summary and next steps

Key points

- Multiple types of hybrid X.509 certificates → analysis paralysis
- IETF protocols are widely used in OT, but OT is not a priority for IETF

What to do

- Develop architecture and use-case documents guiding migration to PQC
- Read and comment [whitepaper about X.509 hybrid formats](#)
- Be open to OT-specific profiling of IETF protocols

Hendrik Brockhaus

Senior Key Expert

hendrik.brockhaus@siemens.com

Alexander Railean

Senior Research Scientist

alexander.railean@siemens.com

Bonus slides

OT uses many protocols defined at the IETF

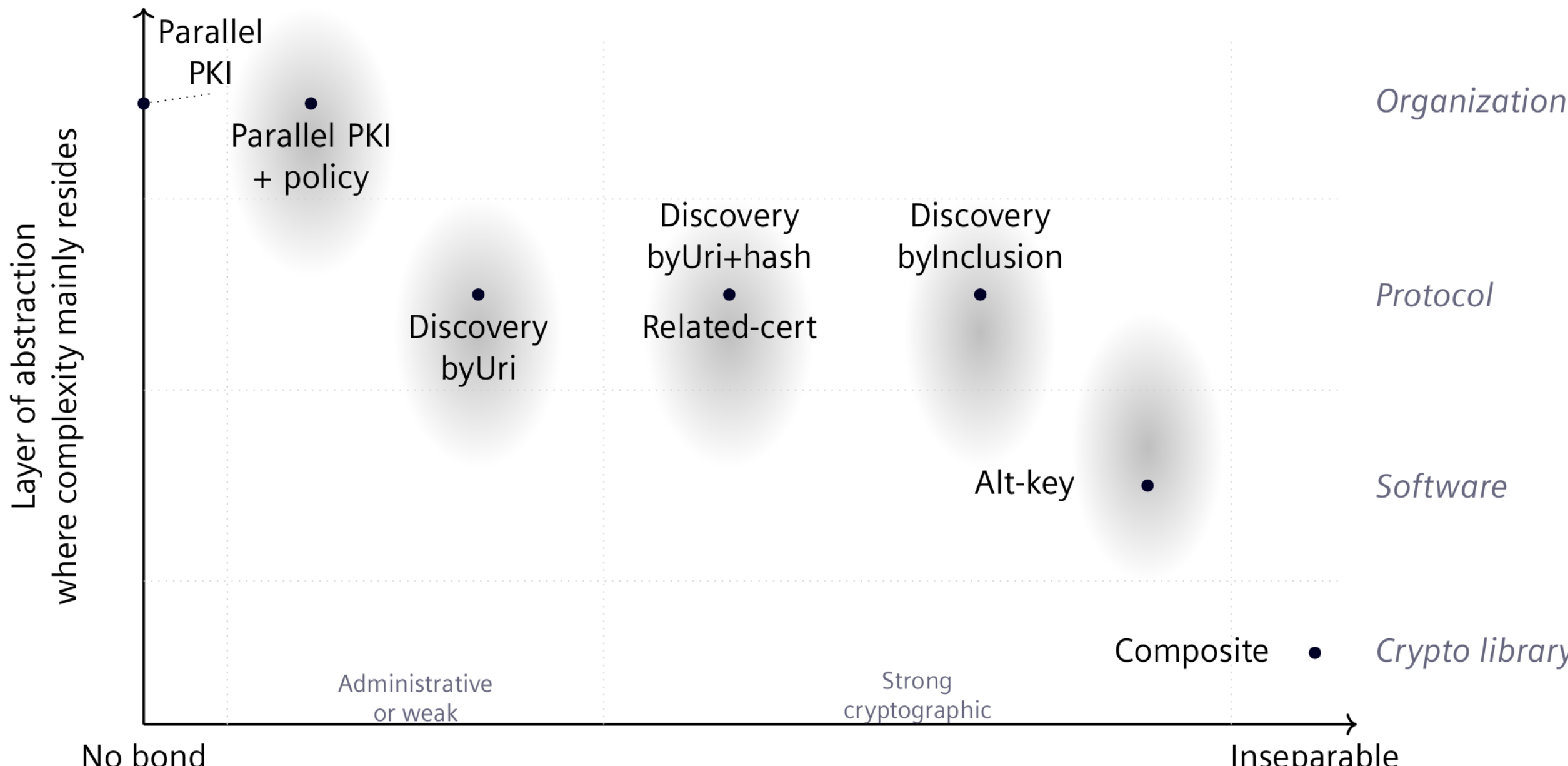
Examples of OT protocols:

- OPC UA
- PROFINET
- IEC 61850 secured by IEC 62351
- IEC 60802 (TSN-IA)
- UNISIG Subset-137
- EU-Rail Security Pillar
- ...

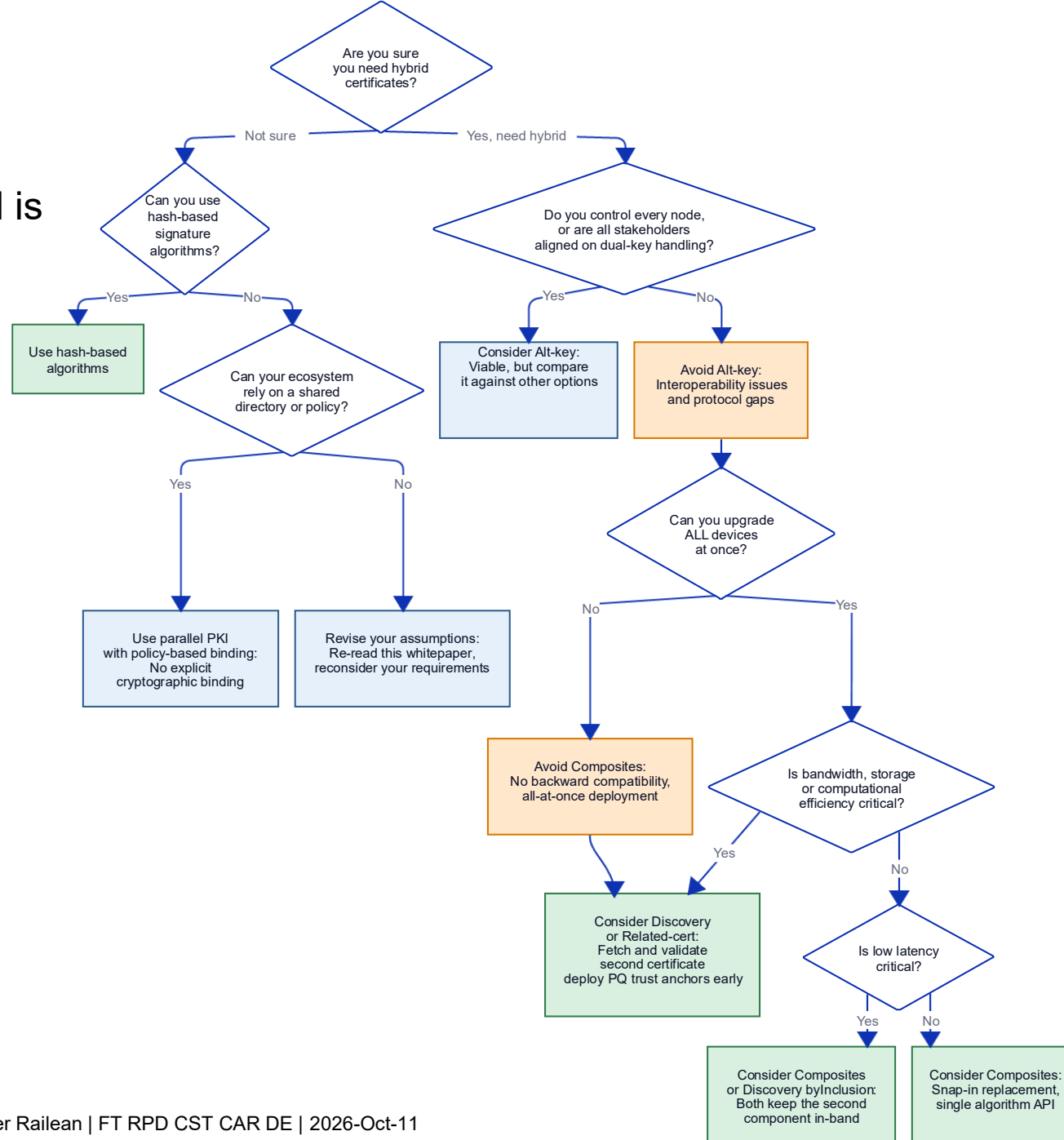
IETF building blocks some OT protocols use:

- | | |
|------------------|-------------|
| • IP, TCP, UDP | • SSH |
| • TLS, IPSec | • NETCONF |
| • X.509/RFC5280 | • JOSE/COSE |
| • HTTP, CoAP | • NTP, SNTP |
| • EAP | • OAUTH |
| • CMS | • SNMP |
| • CMP, EST, SCEP | • Syslog |
| • LDAP | • ... |
| • RADIUS | |

Hybrid certificate formats target different layers of abstraction and separability properties



The tree is *incomplete* and is only a *starting point* for a discussion!



Examples of guiding questions

1. Is there full control every node in the ecosystem?
2. Can all interacting devices be upgraded at once?
3. Is bandwidth, storage or computational efficiency a critical concern?
4. Is network connectivity guaranteed?
5. Do you operate a networked, latency-insensitive system?
6. Is there an external recommendation favouring a specific approach?
7. Have the setup and ongoing operational cost of the chosen approach been accounted for? (e.g., having a parallel PKI)
8. If regulations apply, would the chosen approach qualify as “hybrid” in the eyes of the regulator?
9. Which algorithms have been chosen?
10. Are the chosen algorithms supported by the certificate management infrastructure?
11. What is the scope of use for the certificates, and how likely is scope creep to invalidate the current assumptions?
12. How will trust anchors be distributed: baked-in at manufacture, or updatable? Will certificate pinning be used?
13. If two certificates are not cryptographically bound, how can one ensure both belong to the same entity?
14. Will the traditional and post-quantum certificates share the same lifecycle (e.g., validity period, revocation), or can they diverge?