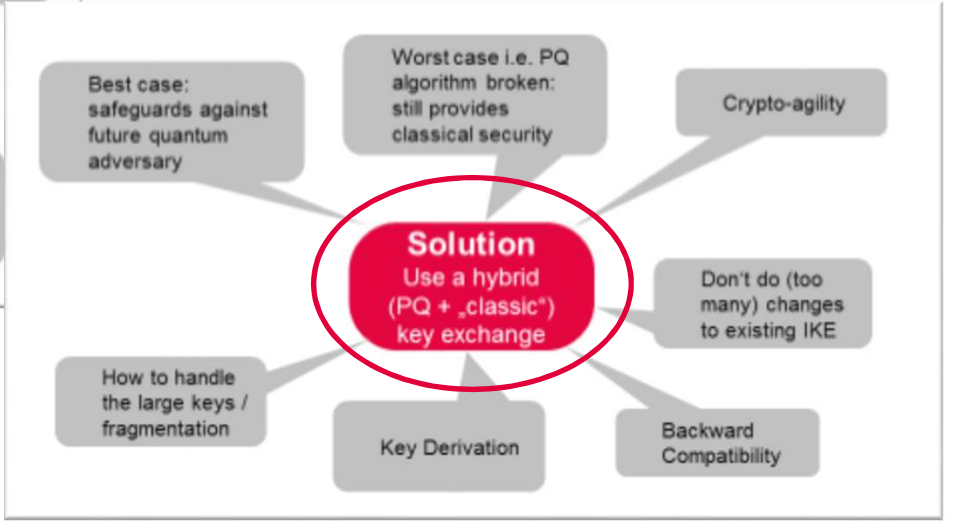
Motivation



+ Kenny Paterson's presentation at SAAG

secunet

Some variation of Cen‘s draft

- **The Fragmentation issue**
  - Will most probably occur for all PQ-safe key agreement protocols
  - IKE over TCP would be a debatable alternative, but … (DoS; designed as a fallback mechanism)
  - → Pro’s and Con’s to move the QSKE to IKE_AUTH exchange
    - Good enough to have PQ-safe CHILD_SA’s? Do we need QSKE for PFS anyway (at this time)?
    - Large initial messages bad for other reasons?

- **The signalling issue**
  - New Transform Type for a PQ safe agreement…
    - Better fits to semantics of transforms, but might need additional logic to deal with multiple / combined KE transforms; btw. KE payload refers to a Transform **ID** only (uniqueness issue)
  - **OR** new Transform Type for a “combined” method
    - Eventually fits better for backward compatibility (PQ choice MUST be combined with DH choice)
  - **OR** both to phase out non-PQ agreements sometimes