• Guardtime AS
  - KSI block-chain
  - BLT signature scheme
  - Verifiable business process (VBP) platform
  - Ahto Truu, ahto.truu@guardtime.com

• Topics proposed
  - Comparison of sparse Merkle trees (SMT) against other authenticated data structures
Review of Authenticated Data Structures

- **Merkle trees (MT)**
  - Aggregate number of inputs to one root hash
  - Provide compact proofs of inclusion

- **Sparse Merkle trees (SMT)**
  - Additionally provide proofs of exclusion

- **Competing structures**
  - Prefix hash tree, Patricia hash tree, ...

- **Task**
  - Compare SMT against others in various usage patterns
  - Evaluate public implementations in Go and Java