Cryptographic Cloud Storage: a proposal

Seny Kamara, Kristin Lauter

Cryptography Group

Microsoft Research

Applications/Scenarios

- Secure Outsourcing for Business
- Electronic Health Records
- Interactive Scientific Publishing
- Electronic discovery
- Regulatory compliance
- Geographic restrictions
- Subpoenas
- Data retention and destruction

Cryptographic Components

- Searchable Encryption (SSE)

[Song, Wagner and Perrig 2000] [Goh 2003], [Chang and Mitzenmacher 2005] and [Curtmola, Garay, Kamara, Ostrovsky 2006]

- Proofs of Storage

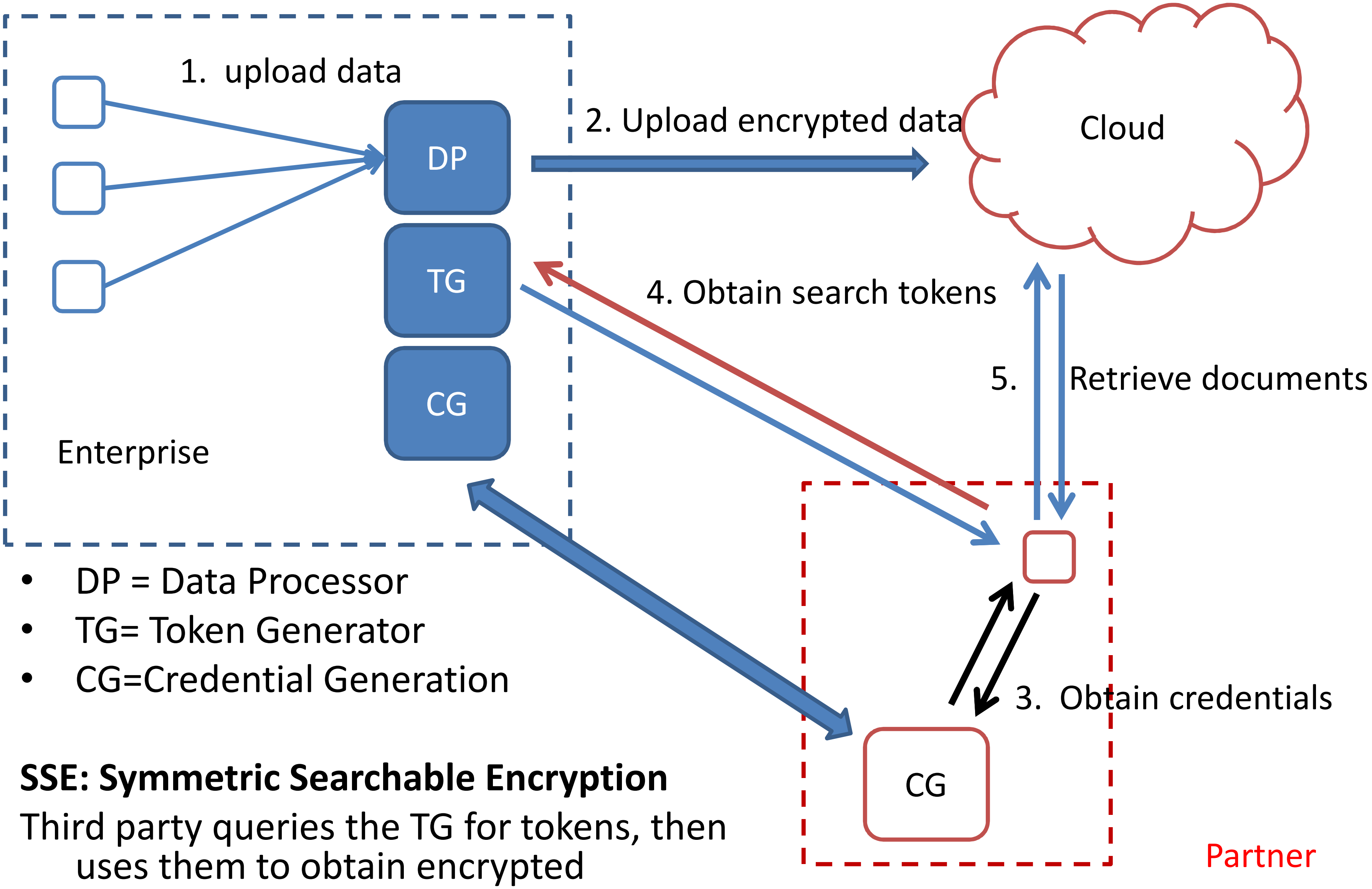
[Ateniese, Burns, et al. 2007], [Juels, Kaliski 2007], [Shacham and Waters 2008], [Ateniese, Kamara, Katz 2009], [Erway, et al. 2009]

- Attribute-Based Encryption

[Sahai,Waters 2005], … , Multi-authority [Chase 2007], [Chase, Chow 2009]

- Authorization Language (SecPAL)

[LaMacchia et al 2007]



- DP = Data Processor
- TG= Token Generator
- CG=Credential Generation

SSE: Symmetric Searchable Encryption

Third party queries the TG for tokens, then uses them to obtain encrypted documents from the cloud