



MLS Architecture: analysis of the security, privacy and functional requirements

Benjamin Beurdouche

► To cite this version:

Benjamin Beurdouche. MLS Architecture: analysis of the security, privacy and functional requirements. 2020. hal-02439526

HAL Id: hal-02439526

<https://hal.inria.fr/hal-02439526>

Preprint submitted on 14 Jan 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

MLS Architecture

Preliminary analysis of the security, privacy and functional requirements

Benjamin Beurdouche

January 14, 2020

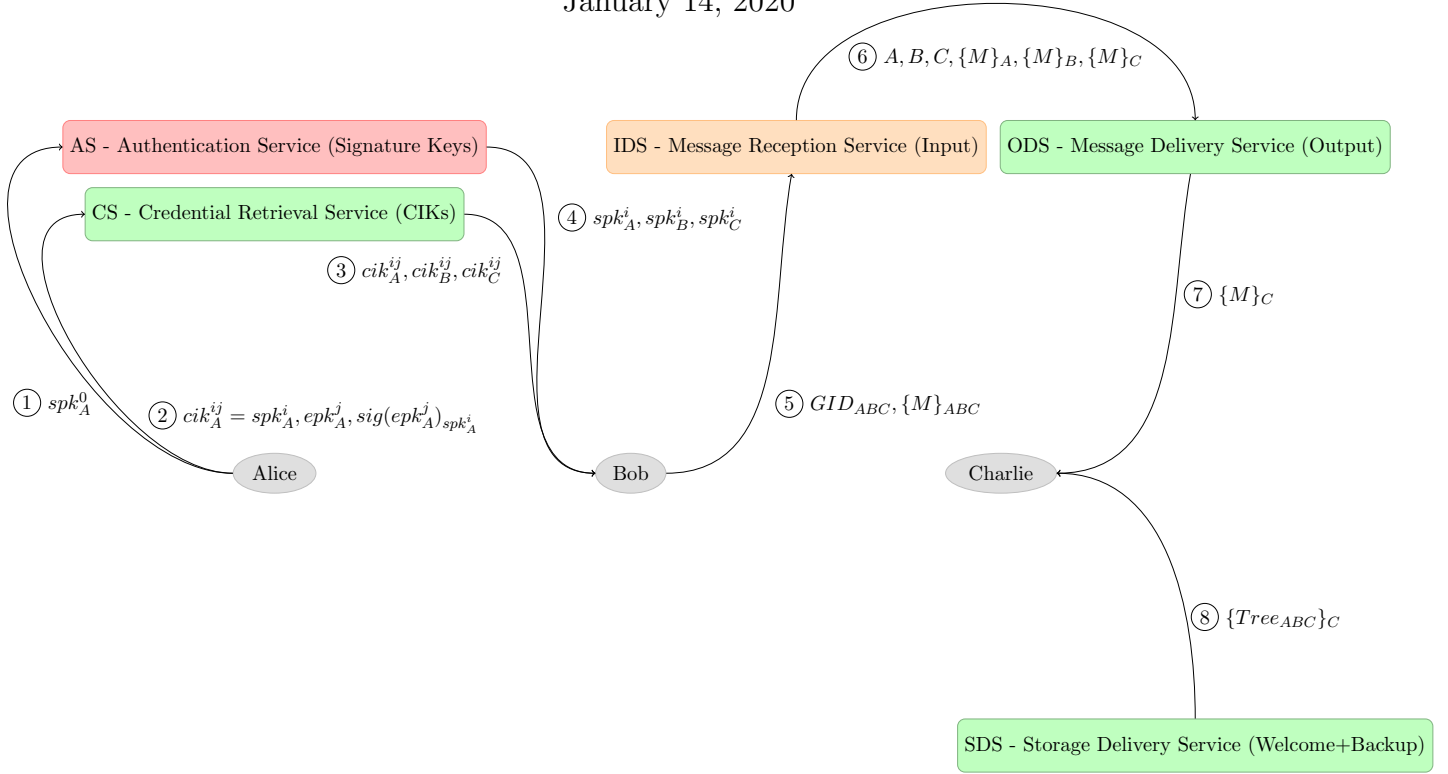


Figure 1: Example of MLS Architecture:

Services trusted for security, privacy and functionality

Services trusted for privacy and functionality

Services trusted for functionality (privacy can still be broken by looking at request patterns)

Description of a data flow within a typical infrastructure:

- ① Alice provides a binder between her identity and a public signature key to the AS
- ② Alice provides her CIKs signed by the authenticated key to the CS
- ③ Bob retrieves CIKs for Alice and Charlie at the CS
- ④ Bob retrieves the signature public keys for Alice and Charlie and authenticates their CIKs
- ⑤ Bob sends a message to the Group ABC to the IDS
- ⑥ The IDS maps the Group Identifier to a list of Members and anonymizes the MLS Ciphertext Header before providing the identity of the recipient and the anonymized messages
- ⑦ The ODS stores the randomized messages for Charlie and forget the recipients, then wait until the message is requested
- ⑧ Charlie retrieves the encrypted public data from the SDS

Description of the knowledge persisted and observed within this infrastructure:

1. AS - Authentication Service

Security: The AS has the link between the identity and the signature key, potentially it may have the ability to generate such links depending on the concrete infrastructure.

Privacy: It may reconstruct parts of existing or future groups depending on requests from clients.

2. CS - Credential Retrieval Service

Privacy: The CS does store the CIKs and may reconstruct parts of existing or future groups depending on requests from clients.

3. IDS - Message Reception Service

Privacy: The IDS has to map final recipients to group members, it can keep this information encrypted or might receive it from the client. Additionally it has to anonymize the header of messages received to make them unique to each recipient. Either the list or the key needs to be “forgotten” by the IDS after processing. A goal is to make sure that the IDS cannot prove group membership but only make a claim.

4. ODS - Message Delivery Service

Privacy: The ODS stores the randomized messages for recipients, it has knowledge of the recipient identity and the association with its push token. It may reconstruct parts of existing or future groups depending on interactions with the IDS.

5. SDS - Storage Delivery Service

Privacy: The SDS stores E2E encrypted data or metadata for groups. It may reconstruct parts of existing or future groups depending on requests from clients.