ChatSecure Push

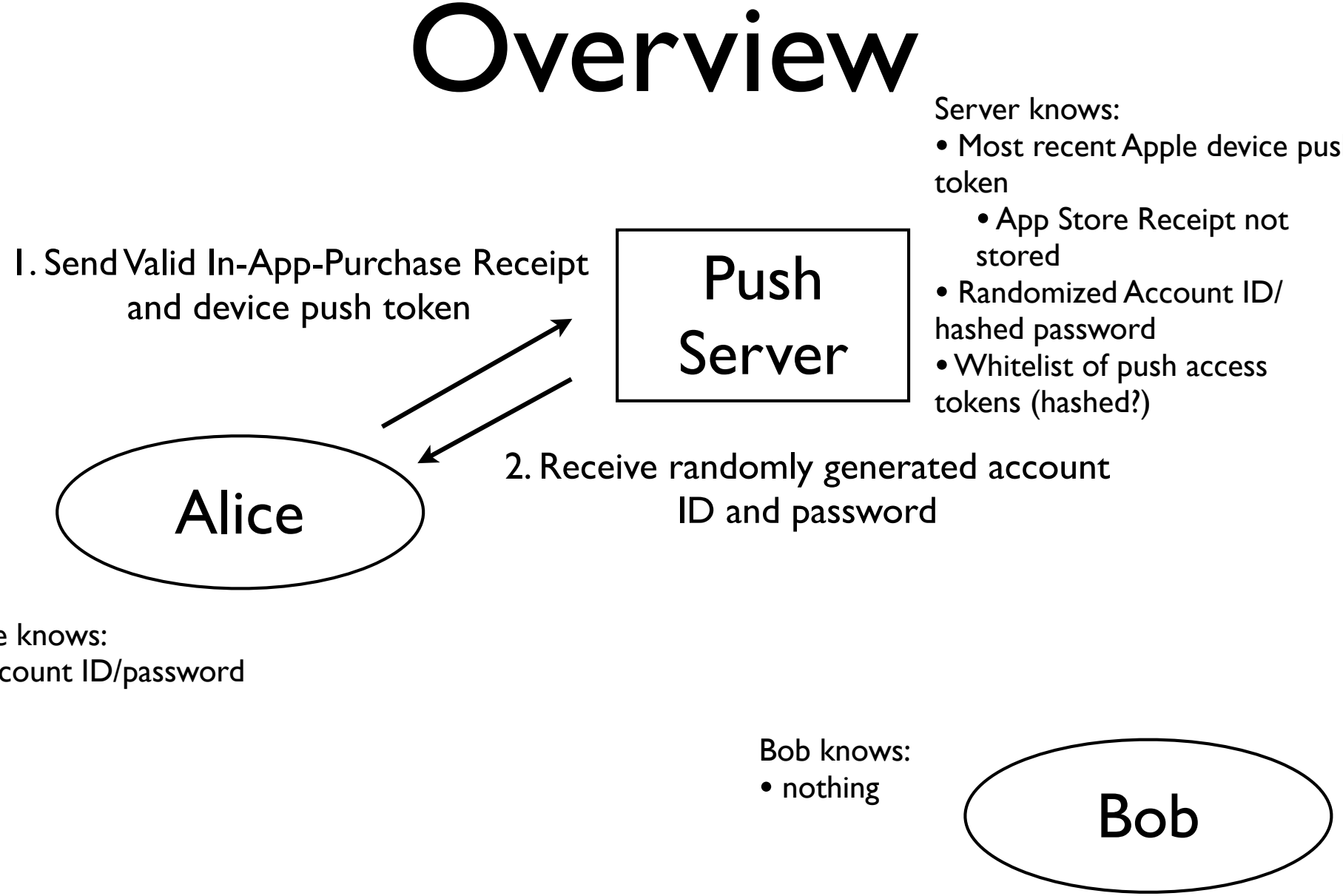
chatsecure.org

©2012 Chris Ballinger

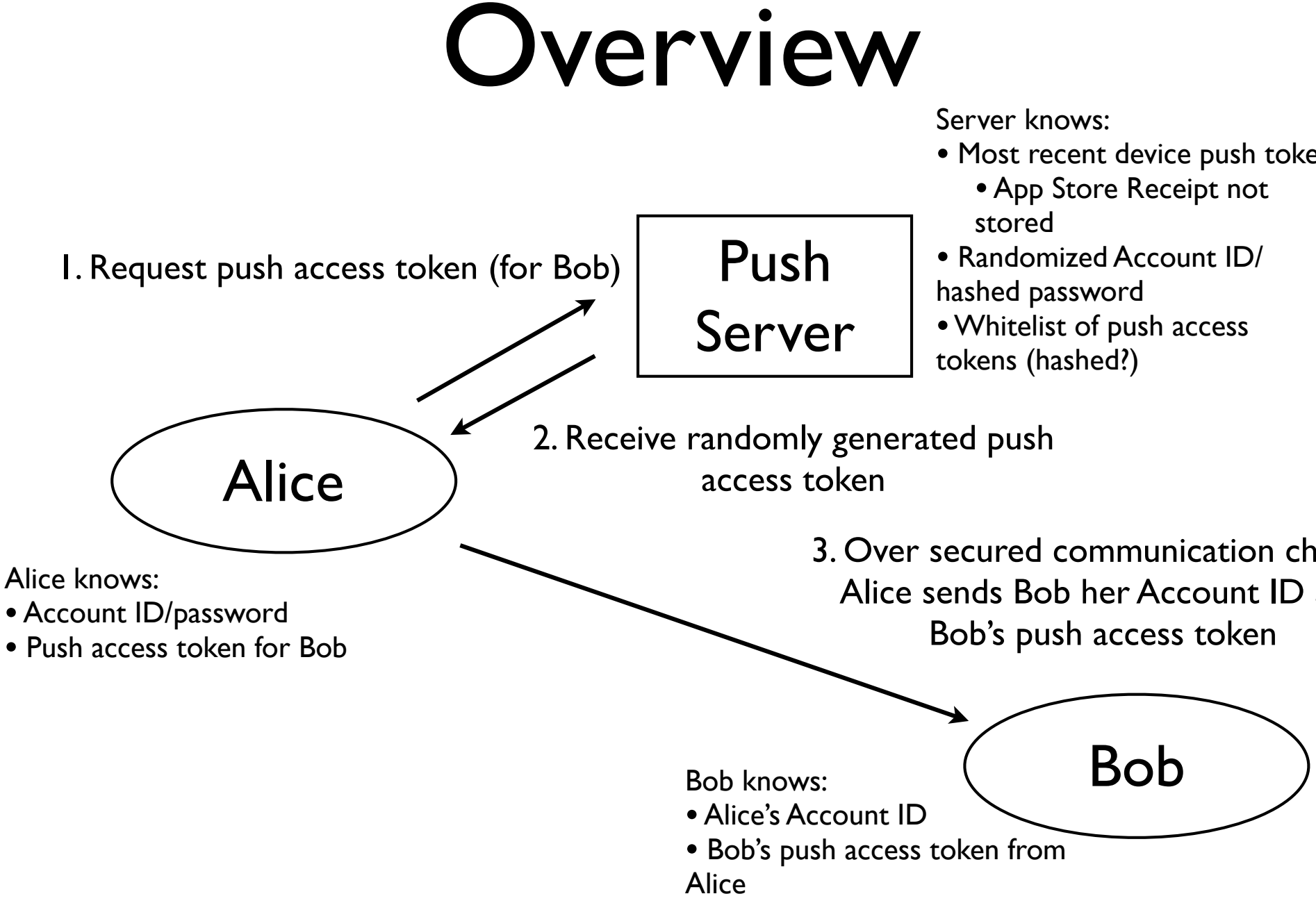
Overview

- Alice is offline, but Bob wants to hold conversation over OTR
- Initial setup:
  - Alice registers with push server via valid in-app purchase receipt to receive randomly generated account ID and password
  - Alice requests a unique push access token (for Bob) from our server and sends PAT & her account ID to Bob over secure communication channel

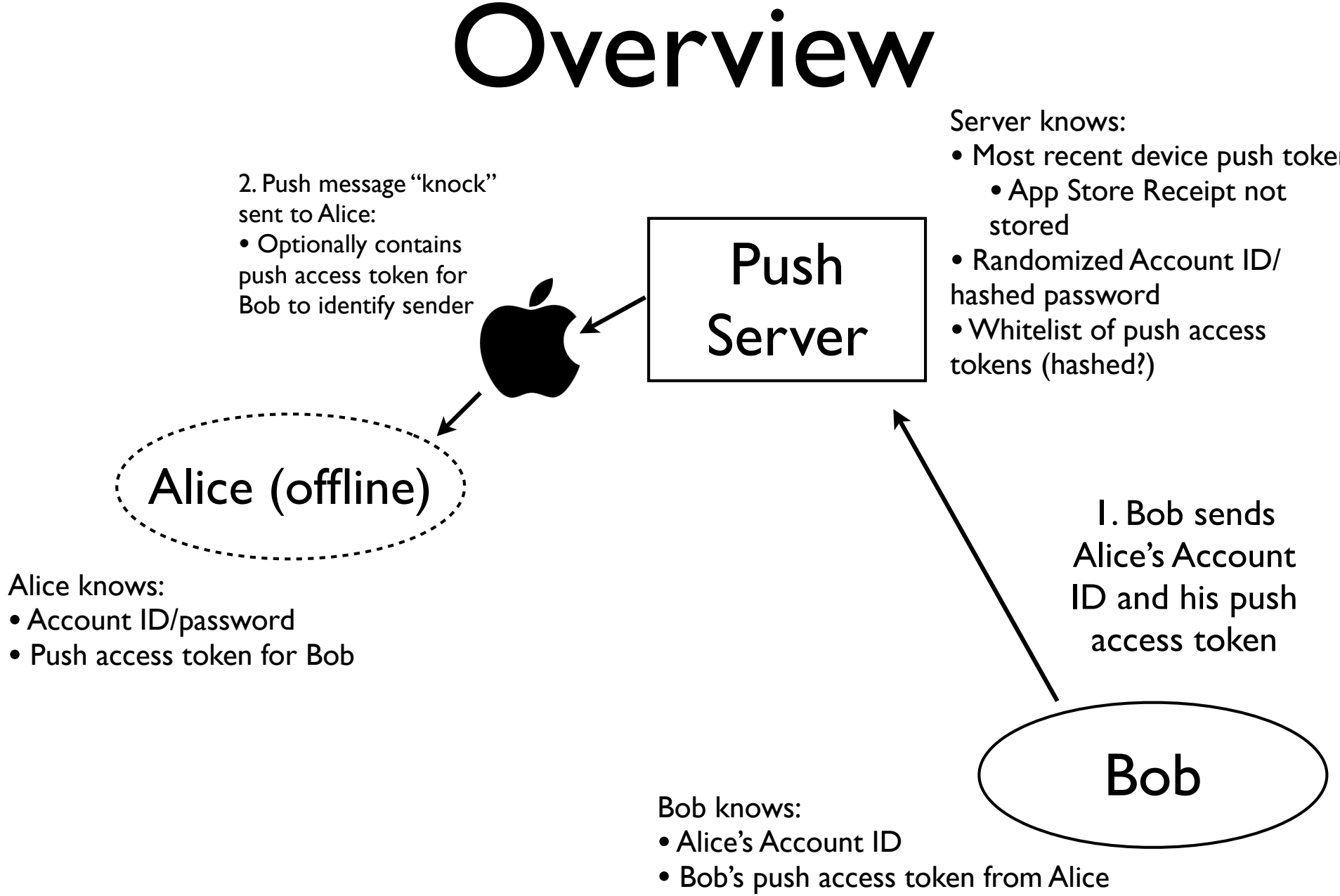
Overview


Server knows:
• Most recent Apple device push token
• App Store Receipt not stored
• Randomized Account ID/ hashed password
• Whitelist of push access tokens (hashed?)
1. Send Valid In-App-Purchase Receipt and device push token
Push Server
2. Receive randomly generated account ID and password
Alice
Alice knows:
• Account ID/password
Bob knows:
• nothing
Bob

Overview


Server knows:
• Most recent device push token
• App Store Receipt not stored
• Randomized Account ID/ hashed password
• Whitelist of push access tokens (hashed?)
1. Request push access token (for Bob)
Push Server
Alice
2. Receive randomly generated push access token
Alice knows:
• Account ID/password
• Push access token for Bob
3. Over secured communication channel Alice sends Bob her Account ID and Bob's push access token
Bob
Bob knows:
• Alice's Account ID
• Bob's push access token from Alice

Overview


2. Push message "knock" sent to Alice:
• Optionally contains push access token for Bob to identify sender
Push Server
Server knows:
• Most recent device push token
• App Store Receipt not stored
• Randomized Account ID/ hashed password
• Whitelist of push access tokens (hashed?)
Alice (offline)
Alice knows:
• Account ID/password
• Push access token for Bob
1. Bob sends Alice's Account ID and his push access token
Bob
Bob knows:
• Alice's Account ID
• Bob's push access token from Alice

Key Features

- Bob doesn't necessarily need to pay to send Alice a push message "knock"
- Payment is only required if you wish to receive notifications
- Protocol agnostic, server knows almost nothing

Glossary

- Push Token: Unique (changing) device token returned from APNs to identify a device
- Push Access Token: Generated by our server, linked to an account ID, acts as a whitelist.