ASSURED
SECURITY CONSULTANTS

PUBLIC STATEMENT

Project	Version nr
Public statement on review of Salt Channel V2 Specification	1.0

Author (Name/Area)	Creation date	Change date
Peter Magnusson Assured AB	2018-02-05	2018-02-05

Salt Channel V2 protocol specification[1] has been reviewed by Assured AB in January 2018. The review was commissioned by the specification's publisher, ASSA ABLOY Shared Technologies / PPI. This is a short public statement on the findings reported in the review.

On a high level, Salt Channel V2 appears to be a secure protocol and meet all of the goals stated in the specification. The encryption provided by NaCl and its application in Salt Channel V2 appears sound. No major breaking security flaw has been found in part of this review.

The following high-level considerations was raised in the review;

- Specification should clarify error handling; it is described under Session Close as closing the Salt Channel session upon any unexpected value; but for different packets there is a lack of clear **MUST** or **SHOULD** requirements for triggering the error handler and when not to.
  - Example: how to handle when received M3_ServerSigKey is different from requested M1_ServerSigKey (OPT).
  - Example: how to handle "Zero. Bits set to 0" received non-zero.
- Time and Delay attack prevention should clarify its requirements on implementations, e.g.:
  - That non-compliant unencrypted client that leaks client real time clock **MUST NOT** be accepted by compliant implementations to enforce the stated goal of "Tracking of the client is impossible.". I.e. if M1 time does not equal to 0 or 1 implementations **MUST** trigger error handler.
  - Recommended threshold, for example max 10 second delay.
  - Maximum acceptable real time clock (RTC) drift per day.

These and other considerations in the full report may be useful for clarifying the specification. A clear specification along with other clients rejecting non-compliant peers may help prevent implementations that interpret the specification insecurely from becoming part of the Salt Channel V2 ecosystem.

[1] https://github.com/assaabloy-ppi/salt-channel/blob/058754c6680a86204d3cebda4feece253a12d40f/files/spec/salt-channel-v2-final1.md