GSATB-98: GAT: Salt Padding Clarifications

The G2S Technical Committee wishes to provide the clarifications detailed in the following pages to implementers of the GAT protocol.

The clarifications in this Technical Bulletin have an impact on GAT 4.0 certification.

Chapter 4 Special Functions

4.2 Defined Special Functions

4.2.4 Special Function: doVerification name algorithm parameters

4.2.4.5 Using Offsets

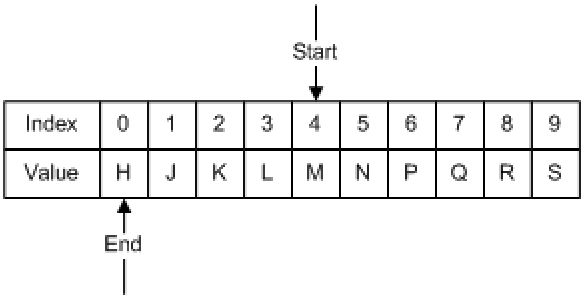
Clarified the requirements for padding salt values.

When supported by an algorithm, offsets may be used to refine the portion of the component that should be verified. Offsets can be used to identify a subset of the component that should be verified, as well as a starting position from which the verification algorithm should wrap around.

When zero-based buffer indexing is used by an implementation, the starting offset identifies the first byte to be included in the calculation. The ending offset identifies the byte at which the calculation stops; that byte is not included in the calculation. If the ending offset is less than or equal to the starting offset, the algorithm wraps around.

For example, to verify the final 6 bytes of the 10-byte buffer containing the ASCII string "HJKLMNPQRS", the starting offset should be set to 4 and the ending offset should be set to 0 (or 10). The buffer to hash would be "MNPQRS".

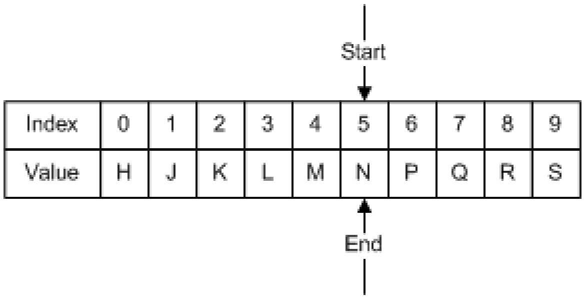
Figure 4.2 Verifying Final 6 Bytes of Buffer Containing "HJKLMNPQRS"



Index	0	1	2	3	4	5	6	7	8	9
Value	H	J	K	L	M	N	P	Q	R	S

To verify the entire 10-byte buffer containing the ASCII string "HJKLMNPQRS" starting in the middle, the starting offset and the ending offset should both be set to 5. The buffer to hash would be "NPQRSHJKLM".

Figure 4.3 Verifying Full 10-byte Buffer Containing "HJKLMNPQRS"



Index	0	1	2	3	4	5	6	7	8	9
Value	H	J	K	L	M	N	P	Q	R	S

Certain algorithms may support a salt value. When supported by an algorithm, the salt value MUST be prepended to the component buffer. The salt value ~~MAY~~MUST NOT be padded or otherwise adjusted before it is prepended to the component buffer ~~when~~unless required by the algorithm.~~ The resulting salt value MUST be hashed before any of the bytes from the component buffer regardless of any offsets.~~

For example, for the 10-byte buffer containing the ASCII string "HJKLMNPQRS", if the client system specifies a 3-byte salt value that is equivalent to the ASCII string "TVW" (no padding or other adjustments required) with a starting offset and an ending offset 4, then the entire 13-byte buffer to hash would be "TVWMNPQRSHJKL".