High-Integrity Device Authentication at Internet Scale

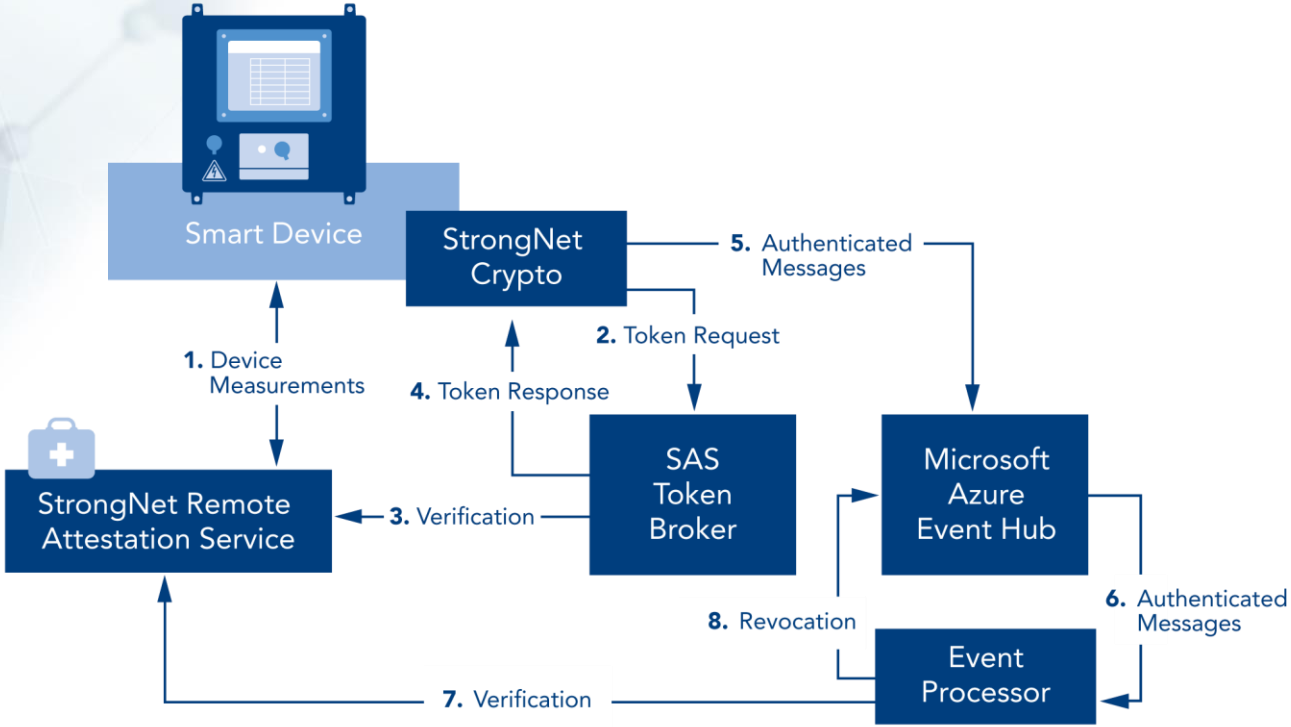
We know security technology, so you know who, when and why.

StrongNet™ secures your critical data and mobile devices.

- **Block sophisticated attacks,** including root kits and pass the hash
- **Enforce encryption** to protect data at rest and in transit
- **Manage device integrity** though interoperable, standards-based secure boot and device attestation

JW secure

We know security technology, so you know who, when and why.



We know security technology, so you know who, when and why.

The process, explained:

1. Device attempts to create a StrongNet measurement-bound key set
2. Device uses its StrongNet key to sign a token request
3. Token Broker service verifies that the token-request signer is trusted with the attestation service
4. Token Broker returns an Azure Shared Access Signature (SAS) token granting short-term **publish** permission
5. Device uses SAS token and StrongNet key to send authenticated and authorized messages to the event hub
6. Event Processor later reads events from the hub
7. Integrity of sender is verified with any message
8. Any token suspected to be stolen is revoked (optional)

For more information:

- JW Secure StrongNet Secure Admin enterprise solution
- HIISDA/IOT detailed walkthrough
- HIISDA/IOT sample source code
- sales@jwsecure.com

We know security technology, so you know who, when and why.